IMPLEMENTATION OF THE USA PATRIOT ACT: SECTION 212—EMERGENCY DISCLOSURE OF ELECTRONIC COMMUNICATIONS TO PROTECT LIFE AND LIMB

HEARING

BEFORE THE

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

OF THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

MAY 5, 2005

Serial No. 109–14

Printed for the use of the Committee on the Judiciary

Available via the World Wide Web: http://www.house.gov/judiciary

U.S. GOVERNMENT PRINTING OFFICE

21–025 PDF WASHINGTON : 2005

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON THE JUDICIARY

F. JAMES SENSENBRENNER, JR., Wisconsin, *Chairman*

HENRY J. HYDE, Illinois
HOWARD COBLE, North Carolina
LAMAR SMITH, Texas
ELTON GALLEGLY, California
BOB GOODLATTE, Virginia
STEVE CHABOT, Ohio
DANIEL E. LUNGREN, California
WILLIAM L. JENKINS, Tennessee
CHRIS CANNON, Utah
SPENCER BACHUS, Alabama
BOB INGLIS, South Carolina
JOHN N. HOSTETTLER, Indiana
MARK GREEN, Wisconsin
RIC KELLER, Florida
DARRELL ISSA, California
JEFF FLAKE, Arizona
MIKE PENCE, Indiana
J. RANDY FORBES, Virginia
STEVE KING, Iowa
TOM FEENEY, Florida
TRENT FRANKS, Arizona
LOUIE GOHMERT, Texas

JOHN CONYERS, JR., Michigan
HOWARD L. BERMAN, California
RICK BOUCHER, Virginia
JERROLD NADLER, New York
ROBERT C. SCOTT, Virginia
MELVIN L. WATT, North Carolina
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
MARTIN T. MEEHAN, Massachusetts
WILLIAM D. DELAHUNT, Massachusetts
ROBERT WEXLER, Florida
ANTHONY D. WEINER, New York
ADAM B. SCHIFF, California
LINDA T. SÁNCHEZ, California
ADAM SMITH, Washington
CHRIS VAN HOLLEN, Maryland

PHILIP G. KIKO, *Chief of Staff-General Counsel*
PERRY H. APELBAUM, *Minority Chief Counsel*

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

HOWARD COBLE, North Carolina, *Chairman*

DANIEL E. LUNGREN, California
MARK GREEN, Wisconsin
TOM FEENEY, Florida
STEVE CHABOT, Ohio
RIC KELLER, Florida
JEFF FLAKE, Arizona
MIKE PENCE, Indiana
J. RANDY FORBES, Virginia
LOUIE GOHMERT, Texas

ROBERT C. SCOTT, Virginia
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
MARTIN T. MEEHAN, Massachusetts
WILLIAM D. DELAHUNT, Massachusetts
ANTHONY D. WEINER, New York

JAY APPERSON, *Chief Counsel*
ELIZABETH SOKUL, *Special Counsel on Intelligence and Homeland Security*
JASON CERVENAK, *Full Committee Counsel*
MICHAEL VOLKOV, *Deputy Chief Counsel*
BOBBY VASSAR, *Minority Counsel*

CONTENTS

MAY 5, 2005

OPENING STATEMENT

WITNESSES

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

IMPLEMENTATION OF THE USA PATRIOT ACT: SECTION 212—EMERGENCY DISCLOSURE OF ELECTRONIC COMMUNICATIONS TO PROTECT LIFE AND LIMB

THURSDAY, MAY 5, 2005

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON CRIME, TERRORISM,
AND HOMELAND SECURITY
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Subcommittee met, pursuant to notice, at 10:05 a.m., in Room 2141, Rayburn House Office Building, the Honorable Howard Coble (Chair of the Subcommittee) presiding.

Mr. COBLE. Good morning, ladies and gentlemen. The Subcommittee on Crime, Terrorism, and Homeland Security holds an oversight hearing today on the implementation of the USA PATRIOT Act's investigative authority for criminal cases. Section 212 is covered by the sunset provision of the PATRIOT Act. The witnesses will discuss the benefits and problems with section 212 and will provide more detail on how the section works.

With that said, let me provide a short summary of what section 212 does and why the section was included in both the House version that passed unanimously out of this Committee and in the Senate version of the PATRIOT Act.

Chapter 121 of the Criminal Code provides for what is unlawful and what is lawful access to stored wire and electronic communications. These stored communications include voice mail, e-mail, and phone messages, for instance. The Federal Criminal Code makes it a crime to access stored communications unless the access is covered by one of the specified exceptions.

Prior to the enactment of the PATRIOT Act, there was no exception for providers to voluntarily disclose information related to life and limb-type emergencies. There was also a strange disparity in the law as there was an exception for communications providers protecting their rights of property to disclose content information, such as the contents of an e-mail, but there was no exception to disclose non-content information under these same circumstances. Section 212 addressed both of these issues.

I look forward to hearing the testimony from our witnesses today on their support and concern for section 212 and I am now pleased to recognize the distinguished gentleman from Virginia, the Ranking Member, Mr. Bobby Scott.

Mr. SCOTT. Thank you, Mr. Chairman, and I again want to express my appreciation to you for devoting the time and attention to the issue of the sunsetted provisions on the PATRIOT Act by holding this series of hearings that you have held on the provisions, including the hearing today on section 212, which involves emergency disclosures under the act.

Now, what the hearings so far has revealed to me is the extent to which we have eliminated many of the checks and balances to secret access by the Government to private, confidential citizen communications and information. Section 212 and other provisions—with section 212 and other provisions, we have effectively changed provisions designed to protect private information from disclosure without due process to provisions designed to allow or require indiscriminate disclosure of information to the Government, and such disclosures can be made with virtually no detached oversight or any other checks and balances, such as required notice before or after the fact, requiring reporting either to a court or to Congress or to the public, or requiring sanctions or remedies for wrongful acts or abuses.

Moreover, with the liberal information sharing provisions that we have, and other provisions, this secretly acquired information, confidential information, can be spread all over town without the person to whom the information pertains ever knowing about it. Further, there still appears to be no restrictions on how long or by whom the information can be maintained.

We need to hear how many times these authorities have been used where no terrorism or imminent threat was involved, or how many times no criminal proceedings or other actions ensued to show whether or not the intrusions were warranted. We are left to simply trust the Government officials to always do the right thing, at the right time, in the right way, with complete immunity, without having to bother the court, the Congress or the public looking over their shoulder while they're doing it.

And, Mr. Chairman, we should use the information we have gleaned from these extraordinary secret powers that we have authorized to put an ordinary checks and balances, such as notice, court oversight, reporting requirements, sanctions, remedies, and failing to do so would turn on its head not only the Electronic Communications Privacy Act and the intent of the fourth amendment of the Constitution, but the healthy mistrust of Government the Framers of our system intended, as well.

So, Mr. Chairman, we look forward to the testimony of our witnesses on how these extraordinary powers are being used and how we can best provide for the necessary checks and balances that our system calls for and how to work to implement those checks and balances. Thank you, Mr. Chairman.

Mr. COBLE. I thank the gentleman from Virginia, and I'm now pleased to recognize the distinguished gentleman from Michigan, the Ranking Member of the full Judiciary Committee, Mr. Conyers.

Mr. CONYERS. Thank you, Chairman Coble, and to my Ranking Subcommittee Member, Bobby Scott, whose statement I endorse completely.

I started out 24 hours ago supporting a conditional extension of section 212. This morning, I am opposed to even extending it. I want it to sunset.

This is the open door, the crack in the door for almost anything to happen. And this is a provision in the PATRIOT Act that has nothing to do with terrorism. So the provision being sold to Congress as a way to protect our critical infrastructure from terrorists has been a boon to those seeking information on everyday crimes, sidestepping the court system completely, and this section of the PATRIOT Act is not even limited to cases where danger is immediate. It goes too far and in too many cases, especially that have nothing to do with terrorism.

There are no safeguards to ensure that those who scare Internet and phone companies into turning over customer information are doing so only when spending that extra hour to get a warrant is truly impossible. There are not even safeguards after the fact.

And plainly, there is no justification for avoiding judicial review or notice to the target that the so-called emergency is over. Indeed, we afford that courtesy to suspected terrorists under the Foreign Intelligence Surveillance Act after an emergency order is not extended by the FISA court. So I hope that we would extend the same rights to American citizens suspected of a far less crime.

The Department of Justice has yet to explain how this section has helped prevent terror attacks or saved anybody's life or limb from terrorists. Now, we will hear about kidnappings and computer hackers, but it seems to me that this has been a little sleeping problem here that I commend the Ranking Member Scott for putting his finger on, and I am particularly interested in hearing from witness Dempsey about the off-the-books surveillance activity and the increasing storage of communications under control of third parties which could threaten, if not eviscerate, the fourth amendment.

So I'm happy to join you, Chairman Coble, as we listen to the witnesses this morning.

Mr. COBLE. I thank the gentleman from Michigan, and we have been joined, as well, by the distinguished gentleman from Arizona, Mr. Flake.

Gentlemen, it's the practice of the Subcommittee to swear in all witnesses appearing before it, so if you would please stand and raise your right hands.

Do each of you solemnly swear that the testimony you are about to give this Subcommittee shall be the truth, the whole truth, and nothing but the truth, so help you, God?

Mr. MOSCHELLA. I do.

Mr. HULON. I do.

Mr. KERR. I do.

Mr. DEMPSEY. I do.

Mr. COBLE. Let the record show that each of the witnesses answered in the affirmative, and you may be seated.

Again, we have a distinguished panel before us. As Mr. Scott said, we have done this in a very thorough, ongoing way. I think this is our ninth—eighth, our eighth hearing on this subject, so we have plowed the field thoroughly.

And gentlemen, I apologized to last Tuesday's panel for my raspy, gravelly throat. I have fallen victim to the damnable April-May pollen attack, so you all bear with me. I know it doesn't sound very good.

Our first witness today is Mr. William Moschella, the Assistant Attorney General in the Office of Legislative Affairs at the U.S. Department of Justice. Prior to joining the Department of Justice, Mr. Moschella served in several positions in the House of Representatives, including Chief Legislative Counsel and Parliamentarian for the House Judiciary Committee. He is a graduate of the University of Virginia and the George Mason University Law School.

Our second witness is Mr. Willie Hulon, the Assistant Director of the Counterterrorism Division of the FBI. Mr. Hulon began his career as an officer with the Memphis Police Department and joined the FBI as a Special Agent and has served the agency in several capacities, both as an investigator and as a supervisor. Mr. Hulon is a graduate of the Rhodes College and the FBI Academy.

Our next witness is Mr. Orin Kerr, the Associate Professor of Law at the George Washington University School of Law. Prior to his current position, Mr. Kerr worked at the Department of Justice in the Criminal Division's Computer Crime and Intellectual Property Section and in the U.S. Attorney's Office for the Eastern District of Virginia. He served as a law clerk for Judge Garth of the Third Circuit Court of Appeals and for the United States Supreme Court Justice Anthony M. Kennedy. He was awarded his undergraduate degree from Princeton University, a Master's in mechanical engineering from Stanford University, and his law degree from the Harvard School of Law.

Our final witness is Mr. Jim Dempsey, Executive Director of the Center for Democracy and Technology, and before I introduce Mr. Dempsey, I want to thank him. I believe, Mr. Dempsey, is this your third appearance before us?

Mr. DEMPSEY. It's my second, Mr. Chairman, but I appreciate helping you work through these issues.

Mr. COBLE. Well, you are apparently not gun-shy because you came back for another bite. [Laughter.]

It is good to have you with us.

Prior to joining the Center for Democracy and Technology, Mr. Dempsey was Deputy Director of the Center for National Security Studies and also served as an Assistant Counsel to the House Judiciary Committee's Subcommittee on Civil and Constitutional Rights. Mr. Dempsey is a graduate of the Yale University and the Harvard Law School.

Gentlemen, as we have previously advised you all, we try to operate under the 5-minute rule here. We have your testimony. It's been examined and will be reexamined. But if you would keep a sharp lookout on the panels that appear before you, when the amber light appears, that is your warning that the fiddler will have to soon be paid. You'll have a minute to go. Then when the red light appears, that will be your signal that your 5 minutes have elapsed.

It's good to have you all with us. Mr. Moschella, if you will start us off.

TESTIMONY OF THE HONORABLE WILLIAM E. MOSCHELLA, ASSISTANT ATTORNEY GENERAL, OFFICE OF LEGISLATIVE AFFAIRS, U.S. DEPARTMENT OF JUSTICE

Mr. MOSCHELLA. Thank you, Mr. Chairman. I appreciate to be before the Subcommittee today. I want to associate myself with the comments of Mr. Scott. I think the American people would be heartened—should be heartened to see the hard work of this Committee.

I would like to personally recognize and thank two members of your staff, former colleagues of mine. I know a lot of staff has worked very hard in putting this series of hearings together, but particularly the work of Beth Sokul and Bobby Vassar. I know you have recently dubbed him "the Granddaddy," but their hard work is certainly appreciated.

Mr. COBLE. If you'll suspend, Mr. Moschella, before I dubbed him Granddaddy, I got the permission of the Ranking Member. I did not get Granddaddy's permission. [Laughter.]

Mr. MOSCHELLA. I'd also like to indicate that there has been a tremendous amount of hard work at the Department of Justice in responding to the hearing request and the needs of the Subcommittee, and I would like to recognize—and many, many individuals are involved, but I'd like to recognize two in particular. First is Mr. Dave Blake of my office, the Office of Legislative Affairs, and the second is Mr. Matthew Berry. Without these two individuals, the hearings would not have come off as well as they had, and we appreciate their hard work very much.

Mr. Chairman, as you know, 16 provisions of the USA PATRIOT Act are set to expire on December 31, 2005, including section 212, which we are addressing today. The tools contained in the PATRIOT Act have been essential weapons in our arsenal to combat terrorists and criminals alike. For this reason, we strongly urge Congress to reauthorize all provisions of the USA PATRIOT Act that are scheduled to sunset at the end of this year.

Mr. Chairman, you summarized the changes made by section 212. Let me just add an exclamation point on a point that you made.

Section 212 amended the law to permit, but not require, a service provider to disclose either content or non-content customer records to Federal authorities in emergencies involving immediate risk of death or serious physical injury to any person. Notably, this provision does not obligate service providers to review customer communications in search of such imminent dangers, nor does it impose an obligation to disclose records once a provider becomes aware of the emergency. It is purely voluntary authority.

Second, section 212, as you stated, amended the Electronic Communications Privacy Act, or ECPA, to allow service providers to disclose non-content information in an effort to protect their own rights and property. Plainly, section 212 of the PATRIOT Act allows electronic communication service providers to disclose either customer records or the content of customers' communications to a Government entity in any emergency situation that involves immediate death—immediate danger of death or serious physical injury. This is analogous to allowing citizens to tell police that while at-

tending a party at a friend's house, they overheard two people discussing a violent crime they were about to commit.

Furthermore, section 212 works in practice. It has been used often and has already saved lives. I'll give just a few examples.

Section 212 was utilized recently in a case involving a series of e-mail threats against an Islamic mosque located in Detroit, Michigan. In this case, Michael Bratisax and John Barnett both allegedly sent threatening e-mail messages on different occasions from their home computers in New York to the Imam of the Islamic Center of America in Detroit. The threats included death to the Imam as well as general threats against all Muslims in America.

The threats were initially reported by the administrator of the mosque to the FBI, and thereafter, the FBI conducted an investigation. During the course of the investigation, due to the life-threatening nature of the e-mail messages, the FBI contacted an Internet service provider who then provided the FBI with the requested information the same day the request was made.

Section 212 permitted the ISP to voluntarily turn over the necessary subscriber information in this case without fear of civil liability, which allowed the FBI to identify Bratisax and Barnett quickly. Both Bratisax and Barnett have been arraigned and charged with the Federal crimes of obstructing the free exercise of religion and transmitting threatening communications in interstate commerce. They are both awaiting trial.

Section 212 has further proven to be extremely useful in cases involving missing children. Section 212 assisted authorities with the rescue of a 13-year-old girl who had been lured from her home and was being held captive by a man she met online. When agents received the report from a local police department that the girl had disappeared the previous day from her parents' home, they did what all agents do. They interviewed the parents, girl's friends, one of whom reported that the girl had discussed leaving home with a 38-year-old man she had met online.

In the next couple of days, an anonymous caller contacted the Bureau and stated that he had chatted online recently with an individual claiming to having taken the girl from Pittsburgh. Based on that information, the FBI agents in Pittsburgh quickly requested information from an ISP pursuant to section 212. With the information provided in response to that request, agents were able to locate the perpetrator. They immediately went to his residence in Herndon, Virginia. At his residence, they rescued the child victim, who was found chained up in his bedroom, and, in his basement, investigators discovered what amounted to a dungeon filled with various torture devices.

The suspect subsequently was arrested, pleaded guilty to charges of traveling with the intent to engage in sexual activity with a minor, and sexual exploitation of a minor, and was sentenced to a prison term of over 19 years. Had the provision of the information by the ISP been slowed, as it would if section 212 were allowed to sunset, who knows what unspeakable horrors this 13-year-old girl would have been subject to by this dangerous predator.

Mr. Chairman, I urge the Committee to lift the sunset on section 212 and all the expiring provisions of the PATRIOT Act and appreciate it.

Mr. COBLE. I thank the gentleman.
[The prepared statement of Mr. Moschella follows:]

PREPARED STATEMENT OF THE HONORABLE WILLIAM E. MOSCHELLA

Statement of
William E. Moschella
Assistant Attorney General
Office of Legislative Affairs
Department of Justice

Before the
Subcommittee on Crime, Terrorism, and Homeland Security
Committee on the Judiciary
United States House of Representatives

Concerning
The Emergency Disclosure Provision of the USA PATRIOT Act (§ 212)

May 5, 2005

Chairman Coble, Ranking Member Scott, and Members of the Subcommittee:

It is my pleasure to appear before you today to discuss section 212 of the USA PATRIOT Act. On September 11, 2001, our Nation suffered a great tragedy. In the wake of this horrendous attack on American soil, we mourned the loss of the thousands of citizens who perished on that fateful day. Almost immediately, the Federal government took steps to prevent such a tragedy from ever happening again. Members of both parties worked to develop comprehensive legislation to achieve four objectives: (1) ensure that law enforcement was provided with the tools necessary to uncover and disrupt terrorist plots; 2) update federal law in light of new information and technology; 3) facilitate information sharing; and 4) safeguard our citizens' civil rights and liberties.

Overwhelming bipartisan majorities in both the House and the Senate passed the USA PATRIOT Act, which was signed into law on October 26, 2001. Since that time, it is difficult to overstate how important the USA PATRIOT Act has been to the Government's ability to preserve and protect our nation's liberty in the face of continuing terrorist threats and serious criminal activity. Thanks in part to this statute, and to the hard work of federal, state and local

law and intelligence investigators around the globe, we have been able to identify terrorist operatives, dismantle terrorist cells, disrupt terrorist plots, and capture terrorists before they have been able to strike.

Sixteen provisions of the USA PATRIOT Act are set to expire on December 31, 2005, including section 212, which we are addressing today. The tools contained in the USA PATRIOT Act have been essential weapons in our arsenal to combat terrorists and criminals alike. We must never forget that terrorist groups pose a continuing and real threat to the safety and security of the American people today. For this reason, I strongly urge Congress to reauthorize all provisions of the USA PATRIOT Act that are scheduled to sunset at the end of this year. We live in a post-9/11 world, and our laws must reflect such circumstances.

Prior to the enactment of the USA PATRIOT Act, Federal law contained no special provisions that would allow electronic communication service providers to voluntarily disclose customer records or communications to Federal authorities in emergency situations. For example, if an Internet service provider (ISP) possessed information that could have prevented an imminent terrorist attack if disclosed to the Government, and the ISP ultimately disclosed the information voluntarily, the ISP could be sued civilly by the customer whose records or communications had been released. Providing such information did not fall within one of the statutory exceptions to the limitations on disclosure contained in the Electronic Communications Privacy Act (ECPA), even if that disclosure was necessary to save lives. Moreover, Federal law did not expressly permit an ISP to voluntarily disclose non-content customer records (i.e. a subscriber's login records) to the Government to protect itself against hacking. The law did, however, allow providers to disclose the content of the customer's communications for this

reason. This created an anomaly in the law – the right to disclose the content of communications should logically imply the less-intrusive ability to disclose non-content records.

Section 212 of the USA PATRIOT Act corrected both of the aforementioned inadequacies. First, section 212 amended 18 U.S.C. § 2702(b)(6) to permit, *but not require*, a service provider to disclose either content or non-content customer records to Federal authorities in emergencies involving an immediate risk of death or serious physical injury to any person. Notably, this provision does not obligate service providers to review customer communications in search of such imminent dangers, nor does it impose an obligation to disclose records once the provider becomes aware of an emergency - it is a purely voluntary authority. Second, section 212 amended ECPA to allow service providers to disclose non-content information in an effort to protect their own rights and property. *See* 18 U.S.C. § 2702(c)(3).

Plainly, section 212 of the USA PATRIOT Act allows electronic communications service providers to disclose either customer records or the content of customers' communications to a government entity in any emergency situation that involves an immediate danger of death or serious physical injury. This is analogous to allowing citizens to tell police that, while attending a party at a friend's house, they overheard two people discussing a violent crime they were about to commit.

Furthermore, section 212 works in practice. It has been used often and has already saved lives. To give just a few examples, section 212 was utilized recently in a case involving serious e-mail threats against an Islamic mosque located in Detroit, Michigan. In this case, Michael Bratisax and John Barnett both allegedly sent threatening e-mail messages on different occasions from their home computers in New York to the Imam of the Islamic Center of America in Detroit. The threats included death to the Imam, as well as general threats against all Muslims in

America in response to events in the Middle East. For example, the e-mails included threats such as: "I have an oath too! It is to kill all you [expletive]"; "I pray to get the opportunity to kill a Muslim"; and "I pray every one of Allahs [sic] followers enjoys hell…that's where you belong. Going to send one myself."

The threats were initially reported by the administrator of the mosque to the FBI and thereafter, the FBI conducted an investigation into the matter. During the course of the investigation, due to the life-threatening nature of these e-mail messages, the FBI contacted an Internet service provider asking the ISP to provide subscriber information immediately. The Internet service provider provided the FBI with the requested information the same day the request was made. Section 212 permitted the Internet service provider to voluntarily turn over the necessary subscriber information in this case without fear of civil liability, which allowed the FBI to identify Bratisax and Barnett quickly.

Bratisax and Barnett have been arraigned and charged with the federal crimes of obstructing the free exercise of religious beliefs and transmitting threatening communications in interstate commerce. They are currently awaiting trial.

Section 212 was used in the investigation of a bomb threat against a high school. An anonymous person, claiming to be a student at the high school, posted a disturbing death threat on the Internet, singling out a faculty member and several students to die by bomb and gun. The operator of the Internet site initially resisted disclosing any information about the suspect to law enforcement for fear that he could be sued if he volunteered the information. Once a prosecutor explained that section 212 allowed for voluntary release of information in emergencies, the owner turned over evidence that led to the timely identification of the individual responsible for the bomb threat. The suspect ultimately confessed to making the threats.

Section 212 was also invaluable in the swift resolution of an attack on a computer that controlled the life support systems for the 50 scientists living at the South Pole Research Station in 2003. Authorities, furthermore, used section 212 to foil an alleged kidnapping plot that turned out to be an extortion racket.

Section 212 and other USA PATRIOT Act authorities were also critical to the safe recovery of an 88-year-old Wisconsin woman who was kidnapped and held for ransom in February 2003. Investigators swiftly used sections 210, 212, and 220 of the USA PATRIOT Act to gather information, including communications provided on an emergency basis from Internet service providers, that assisted in identifying several suspects and accomplices and then quickly locating the elderly victim. When the victim was found, she was bound in an unheated shed during a cold Wisconsin winter several feet from a suspect's residence. Thankfully, the victim fully recovered from her ordeal, which had lasted for several days. Without a doubt, the information obtained using section 212 and other provisions of the USA PATRIOT Act was instrumental in solving the case quickly and thus saving the victim's life. The suspect was eventually arrested and was prosecuted and convicted by Wisconsin authorities after it was determined the victim was not transported across state lines and, thus, could be more effectively prosecuted in state court.

Section 212 has further proven to be extremely useful in cases involving missing children. Section 212 assisted authorities with the rescue of a 13-year-old girl who had been lured from her home and was being held captive by a man she met online. In early 2002, FBI agents received a report from the local police department that the girl had disappeared the previous day from her parents' home. The agents interviewed the parents and the girl's friends, one of whom reported that the girl had discussed leaving home with a 38-year-old man she had

met online. In the next couple of days, an anonymous caller contacted the FBI and stated that he had chatted online recently with an individual claiming to have taken a girl from Pittsburgh. Based on information provided by the anonymous caller, FBI agents in Pittsburgh quickly requested information from an Internet service provider pursuant to section 212. With the information provided in response to that request, agents were able to locate the perpetrator. They immediately went to his residence in Herndon, Virginia. At his residence, they rescued the child victim who was found chained up in his bedroom, and, in his basement, investigators discovered what amounted to a dungeon -- filled with various torture devices. The suspect subsequently was arrested, pleaded guilty to charges of travel with intent to engage in sexual activity with a minor and sexual exploitation of a minor, and was sentenced to a prison term of over 19 years. Had the provision of the information by the ISP been slowed, as it would if section 212 were allowed to sunset, who knows what unspeakable horrors that 13-year-old girl would have been subjected by this dangerous predator.

Some opponents of section 212 argue that ISPs should be prohibited from voluntarily disclosing content and non-content communications of their customers in emergency situations, and should only disclose such information when presented with a court order or grand jury subpoena from the Government. These examples make clear, however, that precious time would be wasted in an emergency situation if a court order or grand jury subpoena were required. For example, in a situation where an ISP becomes aware of an emergency that poses a threat to life and limb, the ISP would first have to contact authorities and provide a sufficient basis for authorities to seek a court order; authorities would then have to obtain the order and serve it on the provider. Only then would the critical information be made available. Requiring such a time-consuming procedure would eliminate the vital benefits provided by section 212 because in

some emergency situations, even a matter of minutes may mean the difference between life and death.

The Department of Justice is called upon each and every day to preserve American lives and liberty. In prosecuting the war on terrorism, the Department has taken every appropriate step to prevent acts of terrorism, protect innocent lives, and respect the civil rights and liberties of every citizen. The USA PATRIOT Act has played a vital role in the Department's efforts to preserve America's system of ordered liberty for future generations. The Department strongly urges Congress to remove the uncertainty that comes with having a "sunset" on criminal and national security law authorities by completely repealing section 224 of the USA PATRIOT Act. Thank you and I look forward to answering any questions you may have.

Mr. COBLE. Mr. Moschella, you put me in a bind. In order to be fair to the other witnesses, I gave you an extra minute, so if you all need 6 minutes, folks, you may take them.

Let me first welcome the gentleman from—the distinguished gentleman from Massachusetts, Mr. Delahunt, has joined us, and the distinguished gentleman from Florida, Mr. Feeney. Good to have you all with us. I think the distinguished lady from Texas was here, Ms. Jackson Lee, but I think she's gone.

Mr. Hulon, good to have you. Hold on just a minute.

Mr. Moschella, I want to thank you for having singled out Beth and Bobby. They have indeed done yeoman's work and they have been assisted by other staffers, too. The staff has contributed very significantly and very tirelessly in this effort and I thank you for acknowledging that.

Mr. Hulon, good to have you with us.

TESTIMONY OF WILLIE T. HULON, ASSISTANT DIRECTOR, COUNTERTERRORISM DIVISION, FEDERAL BUREAU OF INVESTIGATIONS

Mr. HULON. Thank you, sir. Good morning, Mr. Chairman, Ranking Member Scott, and Members of the Subcommittee. It is my pleasure to appear before you today with Assistant Attorney General William Moschella of the Department of Justice, Office of Legislative Affairs, to discuss how the Federal Bureau of Investigations has used the important provisions of the USA PATRIOT Act to better combat terrorism and other serious criminal conduct.

At the Committee's request, I will specifically focus on the emergency disclosure provision of the USA PATRIOT Act, which is scheduled to sunset at the end of this year, and provide you with some examples of how this provision has assisted the FBI's efforts to protect national security. I think you will find this provision has played an instrumental role in helping the FBI fulfill its primary mission of protecting America from further terrorist acts.

Prior to the passage of the USA PATRIOT Act, Federal law contained no special provision authorizing, even in emergency situations, the voluntary disclosure by electronic communication service providers of customer records or communications to Federal authorities. If, for example, an Internet service provider voluntarily disclosed information to the Government, the ISP could have been sued civilly. The Electronic Communications Privacy Act did not contain statutory exceptions which allowed disclosures, even if a terrorist act could be prevented or lives could be saved.

Section 212 of the PATRIOT Act allows a service provider, such as an ISP, to voluntarily provide the content and records of communications related to a subscriber if it involves an emergency related to death or serious injury. Section 212 has been used often and has saved lives.

Many of the emergency disclosures have directly supported FBI terrorism investigations. This provision has also been used to quickly locate kidnapping victims, protect children in child exploitation cases, and respond to bomb and death threats. Because many international service providers are located within the U.S., the FBI legal attaches have also used this provision to assist foreign law enforcement officials with similar emergencies, such as

death threats on prosecutors and other foreign officials. In instances where time is of the essence, giving service providers the authority to voluntarily release information without a court order or grand jury subpoena facilitates the Government's rapid response to crisis situations where the lives of innocent people may be in jeopardy.

I would like to share with you a few examples which illustrate the important role section 212 has played in assisting the FBI in its terrorism investigations.

The first relates to a threat to destroy a mosque in El Paso, Texas. In the spring of 2004, a threatening e-mail was sent to the El Paso Islamic Center. The e-mail warned that if hostages were not released in Iraq, the mosque would be burned to the ground. FBI agents utilizing section 212 were able to quickly obtain information regarding the e-mail from electronic service providers. As a result, Jared Bjarnason of El Paso was identified, located, and arrested before he could carry out this threat. Without the emergency access afforded by section 212, the outcome of this incident may not have been as successful. As it turned out, Bjarnason pled guilty and was sentenced to 18 months in Federal prison.

In another example, many of the details of which are classified, the FBI was attempting to identify and locate suspected terrorists both within the United States and abroad. Utilizing the provisions of section 212, the FBI obtained subscriber information from several Internet service providers based upon a national security need. Subsequently, an individual was identified who was determined to be communicating with a known terrorist organization overseas. Similar results have been repeated throughout many of our field offices and divisions.

Section 212 was used in another FBI terrorism investigation involving attacks against U.S. military forces in Iraq. The investigation determined that a particular terrorist organization was likely responsible for the attacks and might be planning further attacks against additional targets. Pursuant to section 212 of the PATRIOT Act, information was obtained from an Internet service provider which linked individuals in this terrorist organization. The information provided has been invaluable to the FBI and we believe it will help us locate additional subjects in Iraq.

In a final example, section 212 was used in an FBI criminal investigation relating to the murder in Kansas of Bobbie Jo Stinnett, who was 8 months pregnant at the time. Ms. Stinnett was found murdered in her home. Her unborn child had been cut from her body with a kitchen knife. An examination of her home computer revealed that she had been communicating on the Internet in connection with her dog breeding business. A person identifying herself as Darlene Fischer posed as a potential customer. On the same day of the murder, she asked Ms. Stinnett for directions to her residence.

Upon using 212, FBI agents and examiners at the regional computer forensic laboratory in Kansas City were able to obtain information from Internet companies which led to the identification and arrest of an individual whose true name was Lisa Montgomery. Montgomery was arrested and subsequently confessed to the mur-

der. The infant daughter of Mrs. Stinnett was recovered less than 24 hours after the murder.

Some critics have suggested that the computer service providers should not be able to disclose customer records or communications without a court order or grand jury subpoena. The elimination of the provisions of section 212 would severely impact the FBI's ability to respond to certain crisis situations.

First, section 212 allows a service provider to disclose information voluntarily not only when the Government seeks it, but when the service provider itself becomes aware of an emergency that poses a threat to life and limb. To require a court order or a subpoena in such a case would require the service provider first to contact authorities and provide sufficient basis for authorities to seek an order, then would require authorities to obtain that order, and then provide it to the service provider. Real-time implementation of this process would consume precious time in any emergency.

Second, even if in a more unusual case where the Government seeks information from a service provider in response to an emergency, obtaining a court order or subpoena could still take a significant amount of time. In some emergency situations even a matter of minutes can mean the difference between life and death.

In closing, I look forward to discussing with the Committee ways in which the PATRIOT Act has facilitated our ability to conduct terrorism investigations and am happy to answer your questions. Thank you, sir.

Mr. COBLE. Thank you, Mr. Hulon.

[The prepared statement of Mr. Hulon follows:]

PREPARED STATEMENT OF WILLIE T. HULON

Good morning Mr. Chairman, Ranking Member Scott and Members of the Subcommittee. It is my pleasure to appear before you today, with Assistant Attorney General William Moschella of the Department of Justice, Office of Legislative Affairs, to discuss how the Federal Bureau of Investigation has used the important provisions of the USA PATRIOT Act to better combat terrorism and other serious criminal conduct. At the Committee's request, I will specifically focus on the Emergency Disclosure provision of the USA PATRIOT Act, which is scheduled to sunset at the end of this year, and provide you with some examples of how this provision has assisted the FBI's efforts to protect national security. I think you will find this provision has played an instrumental role in helping the FBI fulfill its primary mission of protecting America from further terrorist attacks.

Prior to the passage of the USA PATRIOT Act, federal law contained no special provision authorizing, even in emergency situations, the voluntary disclosure by electronic communication service providers of customer records or communications to federal authorities. If, for example, an Internet service provider ((ISP() voluntarily disclosed information to the government, the ISP could have been sued civilly. The Electronic Communications Privacy Act did not contain statutory exceptions which allowed disclosures, even if a terrorist act could be prevented or lives could be saved.

Section 212 of the USA PATRIOT Act, allows a service provider, such as an ISP, to voluntarily provide the content and records of communications related to a subscriber if it involves an emergency related to death or serious injury. Section 212 has been used often and has saved lives. Many of the emergency disclosures have directly supported FBI terrorism investigations. This provision has also been used to quickly locate kidnaping victims, protect children in child exploitation cases, and respond to bomb and death threats. Because many international service providers are located within the U.S., the FBI Legal Attaches have also utilized this provision to assist foreign law enforcement officials with similar emergencies, such as death threats on prosecutors and other foreign officials. In instances where time is of the essence, giving service providers the authority to voluntarily release information

without a court order or grand jury subpoena, facilitates the government's rapid response to crisis situations where the lives of innocent people may be in jeopardy.

I'd like to share with you a few examples which illustrate the important role Section 212 has played in assisting the FBI in its terrorism investigations. The first relates to a threat to destroy a mosque in El Paso, Texas. In the spring of 2004, a threatening e-mail was sent to the El Paso Islamic Center. The e-mail warned that if hostages were not released in Iraq, the mosque would be burned to the ground. FBI Agents utilizing Section 212 were able to quickly obtain information regarding the e-mail from electronic service providers. As a result Jared Bjarnason, of El Paso, was identified, located and arrested before he could carry out his threat. Without the emergency access afforded by Section 212, the outcome of this incident may not have been as successful. As it turned out, Bjarnason pled guilty and was sentenced to 18 months in federal prison.

In another example, many of the details of which are classified, the FBI was attempting to identify and locate suspected terrorists both within the U.S. and abroad. Utilizing the provisions of Section 212, the FBI obtained subscriber information from several Internet Service Providers based upon a national security need. Subsequently, an individual was identified who was determined to be communicating with a known terrorist organization overseas. Similar results have been repeated throughout many of our field divisions.

Section 212 was used in another FBI terrorism investigation involving attacks against U.S. military forces in Iraq. The investigation determined that a particular terrorist organization was likely responsible for the attacks and might be planning further attacks against additional targets. Pursuant to Section 212 of the USA PATRIOT Act, information was obtained from an Internet Service Provider which linked individuals in this terrorist organization. The information provided has been invaluable to the FBI and we believe it will help us locate additional subjects in Iraq.

In a final example, Section 212 was used in an FBI criminal investigation relating to the murder in Kansas of Bobbie Jo Stinnett, who was eight months pregnant. Mrs. Stinnett was found murdered in her home. Her unborn child had been cut from her body with a kitchen knife. An examination of her home computer revealed that she had been communicating on the Internet in connection with her dog-breeding business. A person identifying herself as Darlene Fischer posed as a potential customer. On the same day of the murder, she asked Mrs. Stinnett for directions to her residence. Using Section 212, FBI agents and examiners at the Regional Computer Forensic Laboratory in Kansas City were able obtain information from Internet companies which led to identification and Lisa Montgomery. Montgomery was arrested and subsequently confessed to the murder. The infant daughter of Mrs. Stinnett was recovered less than 24 hours after the murder.

Some critics have suggested that computer service providers should not be able to disclose customer records or communications without a court order or a grand jury subpoena. The elimination of the provisions of Section 212 would severely impact the FBI's ability to respond to certain crisis situations. First, Section 212 allows a service provider to disclose information voluntarily not only when the government seeks it, but also when the service provider itself becomes aware of an emergency that poses a threat to life and limb. To require a court order or subpoena in such a case would require the service provider first to contact authorities and provide a sufficient basis for authorities to seek such an order, then would require authorities to obtain the order and serve it on the provider, and only then would the critical information be made available. Real time implementation of this process would consume precious time in an emergency. Second, even in the more usual case where the government seeks information from a service provider in response to an emergency, obtaining a court order or subpoena could still take a significant amount of time. In some emergency situations, even a matter of minutes might mean the difference between life and death.

In closing, I look forward to discussing with this Committee the ways in which the USA PATRIOT Act has facilitated our ability to conduct terrorism investigations and am happy to answer your questions. Thank you.

Mr. COBLE. We've been joined by the distinguished gentleman from Texas, Mr. Gohmert, and the distinguished lady from Texas, Ms. Jackson Lee, is back with us. It's good to have you back with us, Ms. Jackson Lee.

Mr. Kerr?

TESTIMONY OF ORIN S. KERR, ASSOCIATE PROFESSOR OF LAW, GEORGE WASHINGTON UNIVERSITY LAW SCHOOL

Mr. KERR. Mr. Chairman, Ranking Committee Member Scott, and Members of the Subcommittee, it's a pleasure to be here today to discuss section 212 of the USA PATRIOT Act, a section that I do support. It's a narrow exception and one quite consistent, even much narrower than similar exceptions in fourth amendment law.

I think if we look at what the PATRIOT Act is trying to do and what the statutory law of electronic surveillance is trying to do, the goal should be to try to match the protections to traditional fourth amendment law, the fourth amendment of the Constitution, which, of course, prohibits unreasonable searches and seizures, and section 212 does exactly that.

It is essentially the exigent circumstances exception to the fourth amendment, which says that law enforcement might ordinarily need a search warrant to, for example, search a house, enter property, seize property, but, if there are competing concerns, whether the destruction of evidence, need to catch a suspect, or some other legitimate law enforcement need, in effect, the courts have allowed a balancing between privacy interests and the competing security interests and said law enforcement can act without a search warrant in an emergency situation.

And section 212 does just that, although actually in a much narrower way. The exception is limited to emergencies. It's limited to protecting human life, serious bodily injury, and, I think, is quite consistent with even narrower than equivalent fourth amendment standards.

Without section 212, this is what has to happen. This is actually what happened at the Justice Department when I was there before section 212, which is that a provider, say an Internet service provider, would contact the Government, and say, "We want to disclose records." The FBI or whatever the agency on the other side would say, "We can't accept those records. We know it makes sense. You should be able to disclose them. But wait, we can't accept them."

The FBI or the law enforcement agency had to then contact the prosecutor. The prosecutor had to obtain a court order, find a judge, get the order signed, serve the order on the ISP, and then that would compel the ISP to disclose what, of course, the ISP wanted to do anyway. It would add a delay of anywhere from a few hours to maybe a day, and I think it didn't really serve a strong law enforcement interest. I think there is a noticed interest, which I will get to shortly, but I don't think it is served by requiring the Government to get a court order to compel a provider to do what that provider wants to do anyway, given the strong, compelling interest.

So, one question is, what is to keep this exception from swallowing the rule? What is to keep an emergency disclosure exception from basically becoming the norm? And I think what keeps that from happening is that privacy is good business. If you are running an Internet service provider, you don't want to disclose a lot of information to law enforcement.

Why? Well, one obvious reason is if information is disclosed, you might get sued. And, of course, you are going to be very worried

if you are, say, at the general counsel's office in the Internet service provider about the policies in terms of working with law enforcement, because as soon as you step over the line of the Electronic Communications Privacy Act, you are subject to civil suit, and that is just bad business. It is bad business not only from the standpoint of getting sued, it is bad business from the standpoint of customer relations. If you are an Internet user, you don't want to go to an Internet service provider that you know might be willy-nilly giving up your information to law enforcement. People like their privacy. So that creates a strong incentive from the ISP perspective not to exploit this exception and to keep the exception narrow.

At the same time, I think there is a legitimate concern about notice, one problem that arises that was mentioned in the prior comments. What's to keep this from being completely secret? Do we want this to be off the books? And I think the fourth amendment is again the proper guide here. Under the fourth amendment, the Government is not required to give notice when an exigent circumstances search occurs. They are required to give notice when they execute a search pursuant to a warrant normally, but not during an exigent circumstances search.

What tends to happen is that the notice is provided and the Government has to then justify its conduct when somebody is actually charged, indicted in court, and then the defense attorney files a motion to suppress under the fourth amendment, saying, "I think that exigent circumstances, sir, was unconstitutional." There's a constitutional suppression remedy, and, of course, the court can then review the search and decide, was this constitutional or not?

What I think needs to change in the Electronic Communications Privacy Act is that some kind of suppression remedy needs to be added to have that occur also in statutory context. What happens now is somewhat odd in that there is no statutory suppression remedy and no constitutional suppression remedy. So say you are an Internet customer whose records have been disclosed unlawfully, whether through a very close call on law enforcement's part or, say, a more egregious violation of the statute. You can't then move to suppress the evidence. A court is not called on to review the Government's procedure. And I think what needs to happen is there needs to be some sort of suppression remedy that allows a defense attorney to make a similar claim the defense attorney would make in the constitutional context.

I think it would be helpful to have, for example, a good faith exception, such as there is in the constitutional context. I'm not saying that there should be a rule that the slightest error means suppression of the evidence, not at all. But there does need to be some sort of way of reviewing the exigent circumstances disclosure beyond the civil remedy, because at least in the experience of the cases on the books, it's just extremely rare for a civil suit to be filed, especially in a criminal case where typically the suspects are going to be guilty. Most people, guilty defendants, don't file civil suits under the Electronic Communications Privacy Act. So a civil remedy, I think, is not the answer and some kind of statutory suppression remedy would really bring the law into alignment with the fourth amendment standard.

Thank you.

Mr. COBLE. Thank you, Mr. Kerr.
[The prepared statement of Mr. Kerr follows:]

PREPARED STATEMENT OF ORIN S. KERR

Testimony of Orin S. Kerr
Associate Professor, George Washington University Law School
United States House of Representatives
Committee on the Judiciary
Subcommittee on Crime, Terrorism, and Homeland Security
Hearing on Section 212 of the USA Patriot Act
May 5, 2005

Mr Chairman, Members of the Committee:

My name is Orin Kerr, and I am an Associate Professor at George Washington University Law School. It is my pleasure to submit this written testimony concerning the USA Patriot Act, and specifically on the emergency disclosure provision found in Section 212 of the USA Patriot Act. My testimony will articulate why I believe Section 212 should be retained. In my view, Section 212 and its analogous provisions for content information are important measures that recognize the need for balance in a regime of electronic privacy, help match statutory law to the contours of the Fourth Amendment, and do not threaten civil liberties. I will begin by offering a broad perspective on the Stored Communications Act and Internet privacy, and then turn specifically to the importance of Section 212 of the USA Patriot Act and its analogous provision for contents.

I. The Goal of the Stored Communications Act

An obvious place to start is by understanding why Internet privacy is a problem for Congress to address. In other words, why are we here today? In most investigations into traditional criminal

offenses, the rules regulating government access to private information are provided by the Fourth Amendment to the United States Constitution. The Fourth Amendment's prohibition against unreasonable searches and seizures regulates police conduct by regulating what spaces the police can enter and what physical property they can take away. Entering a private space such as a home is a Fourth Amendment "search," and taking away physical property is a "seizure." Under existing Supreme Court case law, a probable cause warrant is required to enter a home and retrieve evidence unless an exception such as exigent circumstances applies.

The question is, what changes when we switch from traditional physical crime cases to Internet crime cases? The answer is that computer networks add a third-party intermediary to the picture. Evidence is no longer stored exclusively in the home, but now is often stored with Internet service providers, as well. The police can obtain some information not by entering the home and retrieving physical information, but rather by obtaining information from a suspect's Internet service provider. Under existing Supreme Court caselaw, the Fourth Amendment has a difficult time protecting this information. First, the Fourth Amendment generally offers no protection to information disclosed to third parties, which may very well apply to ISPs. Second, under the "private search" doctrine, private parties such as Internet service providers have unlimited power under the Fourth Amendment to search through documents in their possession and disclose the results to law enforcement. As the Supreme Court stated in *United States v. Jacobsen*, 466 U.S. 109, 113 (1984), the Fourth Amendment "is wholly inapplicable to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any governmental official."

The gap in constitutional protection creates an obvious need for Congressional regulation. In

1986, Congress answered the call by enacting a comprehensive statutory framework as part of the Electronic Communications Privacy Act ("ECPA"), Pub.L. 99-508, 100 Stat.1848 (1986). ECPA erected a complicated statutory regime that generates the equivalent of Fourth Amendment protections on-line by statute. The statute restricts the power of investigators to compel evidence from ISPs and places limits on the ability of ISPs to voluntarily disclose information about their subscribers. The basic goal of the statute is to create Fourth Amendment-like protections for Internet communications. The Stored Communications Act, 18 U.S.C. §§ 2701-11, is an important part of ECPA. Roughly speaking, the Stored Communications Act regulates the exchange of information between ISPs and the government in the case of stored communications and existing account records. The goal of the statute is to restore the kind of limits on government access that might exist under the Fourth Amendment in the analogous setting of physical-world crimes. *See generally* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 George Washington Law Review 1208, 1209-13 (2004).

The emergency disclosure provisions at issue in this hearing concern exceptions to the ban on voluntary disclosure by Internet service providers found in the Stored Communications Act. 18 U.S.C. § 2702 generally bans Internet service providers from disclosing to the government either the contents of customer communications (such as private e-mails) or records relating to customer account usage (such as the e-mail addresses a person sent messages to over a period of time). Section 212 of the USA Patriot Act added an exception to that ban: it provides that an Internet service provider can disclose non-content records to the government "if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information." 18 U.S.C. § 2702(c)(4). In 2002, the Homeland Security Act, Pub.

L. 107-296, slightly modified the preexisting analogous exception for the disclose of contents to the government. The exception is slightly broader for content information than for non-content records; it provides that an Internet service provider can disclose content to the government "if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency." 18 U.S.C. § 2702(b)(8).

II. The Importance and Role of Emergency Disclosure Provisions Under the Stored Communications Act

The emergency disclosure provisions of 18 U.S.C. § 2702(b)(8) and 18 U.S.C. § 2702(c)(4) do not threaten civil liberties, play an important role in a balanced regime of on-line privacy, and match the privacy protections of the Fourth Amendment. Without emergency exceptions such as these, Internet service providers would be barred from disclosing records and contents of communications to the government even when human life is at stake. The law has long allowed ISPs to disclose communications when their legitimate business interests are implicated, *see* 18 U.S.C. § 2702(b)(5), 18 U.S.C. § 2702(c)(3). It would be deeply troubling if the law valued the business interests of ISPs more highly than innocent human lives. The emergency disclosure provisions of 18 U.S.C. § 2702 recognize the commonsense notion that interests in privacy can be outweighed by competing threats to serious bodily injury and life itself.

When might these exceptions be used? Consider two examples. Imagine someone e-mailed a death threat, and the police needed to know who sent the threat to find the wrongdoer or perhaps

to find co-conspirators. The ISP may know this information: they will know who registered the account, and they have access under 18 U.S.C. § 2701(c)(1) to the sender's e-mail account which may reveal the scope of the conspiracy. Without the emergency exception, however, they would be unable to disclose that information to law enforcement. Alternatively, imagine that a kidnaper made a ransom call from a cell phone, and the police wanted to know where the phone was located so they could find the kidnaper and free his victim. Absent an emergency exception, the ISP would be barred by 18 U.S.C. § 2702 from disclosing the location of the cell phone even to safe the life of the victim.

I was a lawyer at the Computer Crime and Intellectual Property Section of the Justice Department from 1998-2001, before the emergency disclosure provision of Section 212 was added, and I remember the prevailing practices within law enforcement at that time. The police and the ISP were forced to rely on an awkward and time-consuming legal fiction to facilitate disclosure. If an ISP contacted government agents seeking to disclose records in an emergency, the following procedures were used: first, government agents would refuse to accept the disclosure, citing the ban in 18 U.S.C. § 2702; second, government agents would go to a lawyer and get the lawyer to apply for and obtain a court order "compelling" the provider to disclose the information under 18 U.S.C. § 2703; third, a judge would sign the court order, compelling the ISP to disclose the information; and then fourth, the agents would inform the ISP that they could finally accept the disclosure. In cases where time was of the essence, this procedure added considerable delay with little to no added benefit.

The emergency disclosure provisions are also consistent with traditional Fourth Amendment principles. One of the traditional principles of Fourth Amendment law is that exigent circumstances can justify taking investigatory steps without first obtaining a court order. *See, e.g.,* Schmerber v. California, 384 U.S. 757, 770-71 (1966). Emergency situations may arise in which the police must

ack quickly. By the time the court order has been obtained, the evidence may be destroyed, the defendant may escape, an innocent person may be hurt, or "some other consequence improperly frustrating legitimate law enforcement efforts" may occur. United States v. McConney, 728 F.2d 1195, 1199 (9th Cir. 1984) (en banc).. In the physical world, this exception permits the police to enter physical spaces and seize physical property under the so-called exigent circumstances exception to the warrant requirement.

These principles can be carried over to Internet crime cases involving ISPs, and are embodied in the emergency disclosure provisions of Section 2702. Granted, the factual picture is a bit different. The privacy invasion is less severe in a number of ways, for example. The police do not enter any physical spaces and do not seize any physical property. The information is held by a third-party provider, and the question is whether that third party can disclose the information voluntarily, not whether the government can forcibly compel the information. In addition, the range of possible threats to safety or law enforcement interests are narrower: exigencies primarily tend to involve harm to an innocent victim rather than the broader set of interests including destruction of evidence that are implicated regularly in traditional exigent circumstances cases.

At the same time, the emergency disclosure provisions in 18 U.S.C. § 2702 are best understood as the Internet equivalents of the traditional warrant exception for exigent circumstances. The police may conduct warrantless searches and seizures under the exigent circumstances exception when a "plausible claim of specially pressing or urgent law enforcement need" exists and that claim outweighs the nature of the privacy intrusion. *Illinois v. McArthur*, 531 U.S. 326, 331 (2001). The analogous statutory exceptions apply when a plausible or good-faith claim of an "emergency" involving danger of "death or serious physical injury" exists and justifies the disclosure. 18 U.S.C.

§ 2702(b)(8), (c)(4). While the test is not exactly the same, the same principle applies translated to the ISP context. The goal is to permit a balancing of interests between privacy and emergency needs. Section 212 and its content equivalent reflects the same balancing effort found in the exigent circumstances doctrine of the Fourth Amendment.

Thank you for providing me with the opportunity to testify.

Mr. COBLE. Mr. Dempsey?

TESTIMONY OF JAMES X. DEMPSEY, EXECUTIVE DIRECTOR, CENTER FOR DEMOCRACY AND TECHNOLOGY

Mr. DEMPSEY. Mr. Chairman, Mr. Scott, Members of the Subcommittee, thank you for the opportunity to testify today.

This series of hearings, and the Subcommittee and the Committee leadership are to be commended for this series of hearings, have offered an unprecedented opportunity to understand the provisions of the PATRIOT Act and how they fit within the context of the electronic surveillance laws. From this kind of detailed, objective inquiry, we can attain the balance that was left aside in the haste and emotion of the weeks after 9/11.

Like many of the provisions in the PATRIOT Act, section 212 is a good idea without sufficient checks and balances. In order to understand what is right and what is wrong with section 212 and similar provisions of the PATRIOT Act, consider what are the three key protections surrounding Government access to private information under the fourth amendment.

First, as a general rule, access to communication should be subject to prior judicial approval.

Second, individuals should have notice when the Government accesses their private data, either before, during, or after the search.

Third, if the Government acts in bad faith, there should be consequences, including making sure that the Government cannot use anything improperly seized, and possibly civil remedies.

These are the three components of a fourth amendment search, and the three are independent: judicial approval, notice, and consequences for bad faith behavior. When it is necessary to create an exception to one of them, that does not mean that it's necessary to create an exception to all three.

For electronic surveillance, Congress has added a fourth protection, namely Congressional oversight and public accountability through routine statistical reporting on how often these techniques are used.

Now, in the case of the emergency disclosures covered by section 212 and described by the Justice Department and the FBI, it is sometimes not possible to obtain prior judicial approval, and the fourth amendment, as Professor Kerr explained, permits exceptions to the warrant requirement in emergency situations. But just because there is an emergency does not mean we have to dispense with the other protections normally accorded by the fourth amendment search.

In the normal warrantless search, at least the search of a home, an office, the person who is the subject of the search is notified of the search, often at the very time of the search. In a traditional emergency, break in the door, the bad guy is there. He is getting the notice. If not, he comes back and should find an inventory or some indication of a search. And if the police act in bad faith during a warrantless search, they cannot use the information they seized.

Under section 212, none of these other protections are available. That's why I call these off-the-books surveillances or off-the-books access. Because the information is held by a third party, there may

be no notice ever to the person whose data is disclosed to the Government. The criminal at least gets notice at trial. The innocent person whose data is mistakenly disclosed to the Government under 212 never receives notice.

And because there is no statutory suppression rule under the historic Communications Act, there may be no consequences for bad faith behavior by the Government. That is why Professor Kerr has called for a statutory suppression remedy. Professor Swire, at an earlier hearing in this series on section 212, also called for that, another emergency disclosure provision.

Finally, we don't even have the oversight of knowing how many emergency disclosures there are. I understand that they may be very large, I've heard from, informally, some people in the industry, especially the disclosure of cell phone location information.

In 2002 in the Homeland Security Act, this Committee mandated a 1-year report from the Justice Department on disclosures of content under section 212. That report was due on November 25, 2003, and as far as I know, it hasn't been submitted yet.

Mr. Chairman, Members of the Committee, we deeply respect the work of the Justice Department and the FBI. They do save lives. But the Justice Department continues to misrepresent the debate before this Subcommittee and before the Congress. Until Congressman Conyers came in this morning, I had not heard anybody calling for the sunset of section 212 or any other provision of the PATRIOT Act. In my view, of course, there should be emergency exceptions. But the debate here is supposed to be over checks and balances, and so far, the Justice Department has refused to engage in that debate, and that's forcing people like the Ranking Member, Mr. Conyers, to move to a position of saying, if we can't insert checks and balances here, if we can't have notice and a reasonable suppression remedy and some accountability to Congress, then maybe this should sunset, and I think that would be a shame because I think there are cases in which this authority is appropriate.

In 2000, Mr. Chairman, this Subcommittee—or this Committee, rather, did take a look at the broader context of the Electronic Communications Privacy Act. It did address some of the changes that would improve the privacy protections, particularly in response to the third-party storage of data which falls outside of various protections, and what we need to do is to create those checks and balances and those protections, giving the Government the tools that it needs but making them accountable.

I look forward to working with you, Mr. Chairman, and the other Members of this Subcommittee and the Committee and with the Justice Department on trying to achieve those checks and balances. Thank you.

Mr. COBLE. Thank you, Mr. Dempsey.

[The prepared statement of Mr. Dempsey follows:]

PREPARED STATEMENT OF JAMES X. DEMPSEY

Chairman Coble, Rep. Scott, Members of the Committee, thank you for the opportunity to testify today. As we said when we testified at an earlier hearing in this series, the Center for Democracy & Technology [1] (CDT) commends the Subcommittee

[1] The Center for Democracy and Technology is a non-profit, public interest organization dedicated to promoting civil liberties and democratic values for the new digital communications

and the full Committee leadership for undertaking these important hearings on the PATRIOT Act. The members of this Subcommittee have devoted considerable time to understanding the provisions of the PATRIOT Act and how they fit within the context of the electronic surveillance laws. From this kind of detailed, objective inquiry, we can attain the balance that was left aside in the haste and emotion of the weeks after 9/11.

CDT's main point in these hearings is that while, of course, the law needs to keep pace with changing technology to ensure that government agencies have access to information to prevent crime and terrorism, those government powers will be no less effective—indeed will be more effective—if they are subject to checks and balances. The law needs to keep pace with changing technology not only to ensure reasonable government access but also to protect privacy, as technology makes ever larger volumes of information available for the government to acquire from third parties, without satisfying traditional Fourth Amendment standards of a warrant and notice. The PATRIOT Act addressed only one side of this equation, making government access easier without counterbalancing privacy improvements. Now is the time for Congress to finish the job and address the privacy side of the equation.

In CDT's view, there is not a single kind of record or communication covered by the PATRIOT Act to which the government should be denied access. The question before us—and it is one of the most important questions in a democratic society—is what checks and balances should apply to government surveillance powers. With respect to the particular PATRIOT section at issue in today's hearing, those time-honored checks and balances should include:

- First, as a general rule, individuals should have notice when the government acquires their communications.
- Second, surveillance techniques should be subject to judicial review, preferably prior judicial approval, but if that is not possible, judicial review after the fact, with sanctions for abuse of the authority.
- Finally, government surveillance needs to be subject to Congressional oversight and some public accountability, including through routine statistical reports.

Section 212 of the PATRIOT Act fails to include these checks and balances.

PREVENTION OF TERRORISM DOES NOT REQUIRE SUSPENSION OF STANDARDS AND OVERSIGHT

At the outset, let me repeat some basic points on which I hope there is widespread agreement:

- Terrorism poses a grave and imminent threat to our nation. There are people—almost certainly some in the United States—today planning additional terrorist attacks, perhaps involving biological, chemical or nuclear materials.
- The government must have strong investigative authorities to collect information to prevent terrorism. These authorities must include the ability to conduct electronic surveillance, carry out physical searches effectively, and obtain transactional records or business records pertaining to suspected terrorists.
- These authorities, however, must be guided by the Fourth Amendment and subject to Executive and judicial controls as well as legislative oversight and a measure of public transparency.

SECTION 212—EMERGENCY DISCLOSURES OF E-MAIL AND OTHER STORED COMMUNICATIONS

This hearing focuses on Section 212 of the PATRIOT Act, relating to emergency disclosures of e-mail and other stored communications. Section 212, like several other electronic surveillance provisions in the PATRIOT Act, has no direct connection with terrorism. It applies not to intelligence investigations, but to all criminal cases.

Section 212 allows the government to tell an Internet Service Provider (ISP) or telephone company that there is an emergency and the ISP or telephone company can then disclose your e-mail, voicemail, or other stored communications without

---

media. Among our priorities is preserving the balance between security and freedom after 9/11. CDT coordinates the Digital Privacy and Security Working Group (DPSWG), a forum for computer, communications, and public interest organizations, companies and associations interested in information privacy and security issues.

even a subpoena, let alone a warrant, and never tell you so that you never have an opportunity to challenge the disclosure.

—Increasing storage of communications under control of third parties threatens traditional Fourth Amendment protections

In our prior testimony, we described the "storage revolution" that is sweeping the field of information and communications technology. ISPs and other service providers are offering very large quantities of online storage for e-mail, documents, and, in the latest emerging services, for voicemail. Increasingly, ordinary citizens are storing information not in their homes but on computer servers, under the control of service providers who can voluntarily or under compulsion disclose the communications and never have to tell the subscribers that their privacy has been compromised.

This technological revolution, coupled with exceptions like Section 212, is eroding Fourth Amendment protections. Traditionally, when records were stored locally, even if there was an emergency justifying an exception to the warrant requirement, you would normally receive notice of the search of your home or office. Yet individuals are never told of Section 212 disclosures unless the evidence is introduced against them at trial. Ironically, under 212, if the e-mail of an innocent person is disclosed by mistake, that person will probably never be advised that the government has obtained their private data.

—"Off the books" surveillance

Section 212 represents another in a steadily growing series of exceptions to the protections of the electronic communications privacy laws. (The computer trespasser provision of Section 217 is another example.) Section 212 and similar provisions essentially allow "off the books surveillance"—they define certain government interceptions not to be interceptions, and certain disclosures to the government not to be disclosures.

Once an access to communications or data is excluded from the coverage of the surveillance laws, not only is it not subject to prior judicial approval, but there are no time limits on the period covered by the surveillance or disclosure, no minimization requirement, no report back to a judge, no notice to the persons who are surveilled unless and until the government introduces the evidence against them in a criminal trial, no suppression rule for violating the statute's standards (no suppression remedy at all if the information is deemed to be outside the protection of the Fourth Amendment), and no reports to Congress and the public.

Emergency exceptions are sometimes reasonable, although in an age when warrants can be obtained by telephone or fax and presumably even by e-mail, see Federal Rule of Criminal Procedure 41(d)(3), and when every court should have a duty judge available by cell phone or Blackberry 24 hours a day, emergency exceptions to judicial oversight should be extremely rare. And they should be subject to checks and balances.

—The potential for government exaggeration of the facts

The crucial thing to recognize about Section 212 is that the information about the emergency will often come from a government agent. Rather than going to a judge and getting a warrant, even if time and technology permitted it, Section 212 permits a government agent to go to a service provider, say there is an emergency, and if the service provider reasonably believes there is (even if the government agent was exaggerating), the service provider can disclose the records with no liability and no notice to the subscriber. Surely, this is an invitation to cutting corners, if not more cynical forms of abuse. Notice also how placing the reasonable belief on the part of the service provider diffuses responsibility: the stored records provisions to which this exception was added has no suppression rule for evidence improperly obtained, and it does not appear that the civil action and administrative discipline provisions of 18 U.S.C. 2707 would apply to agents who even intentionally mislead a service provider about the existence of an emergency.

Other parts of Section 212 are non-controversial: It rearranged sections 2702 and 2703 of title 18 so that section 2702 now regulates all permissive disclosures (of content and non-content records alike), while section 2703 covers compulsory disclosures. Second, an amendment to the new subsection 2702(c)(3) clarifies that service providers have the statutory authority to disclose non-content records to protect their rights and property.

The language of Section 212 covering emergency disclosures of the content of communications was rewritten by the act creating the Department of Homeland Security. In some ways the new language is narrower than the PATRIOT language, while in other ways it is broader (it allows disclosure not only to law enforcement but to any government entity), but our concerns and recommendations about checks

and balances pertain to the new language as well. Also, an uncodified provision of the Homeland Security Act required government entities obtaining the contents of communications under the new emergency exception to report to the Attorney General and the Attorney General to file a one-time report to Congress in November 2003 on the use of the authority. Someone needs to look for that report.

—Recommended amendments to establish checks and balances

Checks and balances should be added to Section 212.

- The person whose privacy has been compromised should be notified that his information has been disclosed to the government. This is especially important in cases of mistake—where the government obtains records on the wrong person, that person should be notified.
- There should be a statutory remedy for abuse, barring the government from using information if it had mislead the service provider into believing there was an emergency. An additional or alternative protection would be to make it illegal for a government official to intentionally or recklessly mislead a service provider as to the existence of an emergency. Coupled with notice, this could provide a reasonable remedy to persons whose privacy was needlessly invaded.
- To permit ongoing oversight, emergency disclosures of stored communications to the government should be reported to Congress in annual, public statistical reports.

THE BIG PICTURE: PROTECTIONS FOR PRIVACY SHOULD BE UPDATED IN LIGHT OF CHANGING TECHNOLOGY

As CDT has noted before, many of the changes in the PATRIOT Act appear small in isolation. However, no consideration has been given in almost five years to other, long-recognized changes that need to be made to strengthen the privacy protections of the electronic surveillance laws, including:

- extending Title III's statutory suppression rule to electronic communications, a change even the Justice Department once supported;
- increasing the standard for pen registers and trap and trace devices, to give judges meaningful oversight, a change the full Judiciary Committee supported in 2000;
- eliminating the distinctions between opened and unopened e-mail and between relatively fresh and older e-mail, by bringing all stored e-mail under a warrant standard, another change the Committee supported in 2000;
- establishing a probable cause standard for access to location information, a change this Committee also supported in 2000;
- requiring reporting on access to e-mail, also supported by the Committee in 2000.

With this context in mind, it is easier to see why even some of the minor changes in the PATRIOT Act draw concern, for they are part of a steady stream of uni-directional amendments that are slowly eroding the protections and limits of the electronic privacy laws.

CONCLUSION

CDT supports the Security and Freedom Enhancement (SAFE) Act, a narrowly tailored bipartisan bill that would revise several provisions of the PATRIOT Act. It would retain all of the expanded authorities created by the Act but place important limits on them. It would protect the constitutional rights of American citizens while preserving the powers law enforcement needs to fight terrorism.

We look forward to working with this Subcommittee and the full Committee as you move forward in seeking to establish some of the checks and balances that were left behind in the haste and anxiety of October 2001.

Mr. COBLE. Now, we apply the 5-minute rule to ourselves, too, gentlemen, so if you all can be as terse as you can when you respond.

Mr. Hulon, the glaring example you gave about the El Paso episode, I presume that the agents could not have responded as quickly as they did prior to the PATRIOT Act, is that correct?

Mr. HULON. That's correct, sir. They were able to get the information in regards to the subject who made the threat and actually go out to make the arrest or make the approach very quickly.

Mr. COBLE. Mr. Moschella and Mr. Hulon, some have argued that because this exception has been used more in the criminal context than the war on terrorism, that it is probably not a good exception. Do you believe this exception is important for crimes of terror as well as for, say, for crimes of kidnapping and murder, *et cetera*? If you will comment on that, Mr. Moschella, I will start with you.

Mr. MOSCHELLA. Thank you, Mr. Chairman. This is a tool that we would use in both terrorism cases and other cases. As the one example that I explained to the Committee, this traveler case of this 13-year-old girl who was brought across State lines for these illicit purposes demonstrates, this is a critical tool to save life and limb. When the Congress originally considered the PATRIOT Act, it knew that it was amending certain statutes that had general applicability for all criminal investigation, and this is a needed tool in those efforts.

Mr. COBLE. Mr. Hulon?

Mr. HULON. Yes, sir. I think it's very important for terrorism investigations. Some of the examples that might be cited, of course, are ones that end in prosecution. But in terrorism investigations, a lot of our work and effort to detect or prevent an act a lot of times does not end up with a prosecution that gets public notification. A lot of it goes with intelligence building that we end up using to further our intelligence base and also to work toward identifying groups and individuals that are in support of terrorism.

Mr. COBLE. I thank you, sir.

Mr. Kerr, you made what I believe is a good point when you indicated it would be troubling if the law valued the business interest of communications providers more highly than protecting innocent human lives. Is that not what 212 addresses? That is, communications providers should disclose content information to protect their property and rights, but no exception prior to PATRIOT, as I understand it, to disclose information that would protect another human being. Comment on that, if you would, Mr. Kerr.

Mr. KERR. Thank you, Mr. Chairman. I think that's exactly right. The Wiretap Act has long had—and the historic Communications Act have long had a range of exceptions recognizing competing interests, whether they are business interests or other interests. And to be honest, when I was at the Justice Department before section 212, it always seemed to me that Congress just had forgotten to add some sort of an exigent circumstances exception. I used to train FBI agents on how the statute worked and I remember having to explain to people, I said, "You know, you're not going to believe it, but currently, the statute has no exception for exigent circumstances like a kidnapping."

And so I think it's an important step forward and clearly a good idea to add section 212. I think it does say there are competing interests and innocent human life is clearly—that's clearly a very strong competing interest that should justify disclosure.

Mr. COBLE. Thank you, sir.

Mr. Dempsey, in your testimony, you state that the crucial thing to recognize about section 212 is that the information about the emergency will often come from a Government agency and you indicate that that might be an invitation to cut corners. But is it not a voluntary disclosure at that juncture?

Mr. DEMPSEY. Mr. Chairman, it is a voluntary disclosure, but I think that the service provider is going to be predisposed to make the disclosure. They have immunity for making a disclosure if they believe, in good faith, that there is an emergency, and they will obviously be predisposed to believe whatever the Government tells them. They cannot be sued civilly if they make the disclosure. They never have to tell their customer that they've made the disclosure. And they, in fact, might face some liability if they don't make the disclosure and somebody ends up injured. So, I think the whole presumption has shifted toward the disclosure with no incentive on the other side.

At some level, the service provider should have—I'm not questioning the service provider immunity when they believe in good faith that there's an emergency. That makes it possible for the Government to come in, breathless, a little bit exaggerating, perhaps, or believing, rightly or wrongly, that there's an emergency when there isn't, and at that point, there's no accountability. There's no accountability, I think, for the Government, because if the Government is misleading, as we have talked about, they suffer no consequences, either.

Mr. COBLE. I thank you, sir. I see my time has expired.

Before I recognize the gentleman from Virginia, I have a physician's appointment, hopefully to help me overcome this malady that you all are having to suffer with me, and I want to thank the panel for being here in case I don't return. I've asked the distinguished gentleman from Florida if he would take the gavel in my absence, and I now recognize the gentleman from Florida—from Virginia.

Mr. SCOTT. Thank you, Mr. Chairman, and I hope you're feeling better.

Let me get a little background where we are. In 1986, we passed the Electronic Communications Privacy Act and that is the act which prohibited electronic ISPs and what not from disclosing information violating your privacy. Prior to that, was there anything to prevent an Internet provider from just voluntarily giving up your private information?

Mr. KERR. Probably not.

Mr. SCOTT. And as a result of the——

Mr. KERR. Other than their terms of service, but——

Mr. SCOTT. A contract?

Mr. KERR. Yes.

Mr. SCOTT. Now, after '86, there was no exception for emergencies?

Mr. KERR. There was an exception for information relating to a crime that was inadvertently discovered. If the ISP inadvertently discovered a threat or information about any crime, they could disclose that, but I think it's correct that there was a little bit of oversight or Congress was not fully—that was the first effort. I think they probably did leave out the emergency exception.

Mr. SCOTT. Now, what is the—is there any problem, Mr. Dempsey, proceeding under the emergency but requiring a warrant as soon as practicable?

Mr. DEMPSEY. Well, that's an interesting point, because under title III, which is the basic wiretap law, not for stored but for live interception, there is an emergency exception. That was created in 1968. And where there's an emergency exception under title III for live interception, the Government must then go and apply for an order after the fact and if the order is denied, it must terminate the surveillance and cannot use anything acquired during the claimed emergency if it turns out that there wasn't justification.

Mr. SCOTT. Is there a poison fruit problem with that information that was acquired in the meantime?

Mr. DEMPSEY. I think they would be prohibited from using it further in their process.

Mr. SCOTT. Mr. Dempsey, you talked about the consequences of failing to—failing to get the information if it was not an emergency and suggested that in bad faith, there should be some consequences. Some of us have a problem with the bad faith, the good faith exception because you can very easily in good faith trample on somebody's rights. And, in fact, the good faith exception gives you a perverse incentive to fail to educate your law enforcement officials and just hire good old boys that just didn't know any better, so they get to court, "I didn't know."

Mr. DEMPSEY. Congressman, I——

Mr. SCOTT. I'm in good faith.

Mr. DEMPSEY. I definitely agree with you or see where you are coming from here. In my recommendations today, I did not want to go back and revisit one way or the other the good faith exception to the exclusionary rule. The statutory suppression rule under title III, under the live interception law, has basically been interpreted to have almost a good faith exception, as well. It is not applied in the case of minor or inadvertent noncompliance. So I was taking the good faith exception as a given here and saying that, at the least——

Mr. SCOTT. In other words, we'll just debate that at another point.

Mr. DEMPSEY. That's what I was saying.

Mr. SCOTT. Okay. One of the problems with the exclusionary rule generally is the safeguard, and, I think, frankly, for the defendant to protect people, the exclusionary rule is the only meaningful sanction that there is. As has been pointed out, suing somebody isn't going to get you anywhere. The court jailing of police officers for messing up a warrant isn't going anywhere. The exclusionary rule actually works because it removes the incentive to mess up.

One of the problems in this case is that if you're not a defendant, you have no standing to complain. Is that, Mr. Moschella, is that right? If they get my information and you're the defendant, I have no—if they illegally got my information and they use it against you, I have no standing. You might have some standing to complain, but I have no standing to complain, is that right?

Mr. MOSCHELLA. Mr. Scott, I think that the determination is a fact-specific one as to whether or not the Frank amendment, it's

the Frank amendment, section 2707 of title 18, does apply to this entire chapter.

If I may add one thing to what Mr. Dempsey added, I am not aware—there certainly is no good faith exception written into the statutory exclusionary rule. In fact, that rule is so strict that if you had two criminals, two co-conspirators who didn't trust each other and were illegally taping each other, so violating the Wire Act, and that information came into the possession of the Government to use against one of them, we would not be able to use it. That's how strict that statutory suppression provision——

Mr. DEMPSEY. I was talking about Government behavior, Congressman.

Mr. FEENEY. [Presiding.] Thank you. The gentleman's time has expired.

The gentleman from Arizona, Mr. Flake, is recognized.

Mr. FLAKE. I thank the Chairman and the witnesses.

With this and other sections of the PATRIOT Act, we often hear from the Department of Justice with regard to whether you need a statute to protect this or that, well, we would never do that, or our agents, FBI agents would never do this or that. Mr. Hulon, can you tell me, have there been instances where FBI agents have been reprimanded or disciplined for filing false affidavits or misleading affidavits before a FISA court or anywhere else?

Mr. HULON. I don't recall that there have been situations where that has occurred recently. I'm just not aware, sir.

Mr. FLAKE. According to Judge Lambert, a FISA court did bar one FBI agent from ever appearing before the court again for filing a series of misleading affidavits. Were you aware of that?

Mr. HULON. I'm not aware of the details on that one, sir.

Mr. FLAKE. Is anyone here aware of that? Mr. Moschella, have you heard of that?

Mr. MOSCHELLA. I'm generally aware of it, yes, sir.

Mr. FLAKE. Okay. Do you know of any action that has been taken against this agent?

Mr. MOSCHELLA. I'd have to check into that.

Mr. FLAKE. Could you get back to my office on that?

Mr. MOSCHELLA. Yes, sir.

Mr. FLAKE. That goes to one of the issues that I think a lot of us have. We're kind of told—the last defense is, "Well, you don't need a statute for that because our agents or this Department just wouldn't do that." But yet we hear of an instance here where that did occur and you're unable to tell us whether that agent was even disciplined. So it would be useful—Mr. Dempsey, can you comment on that?

Mr. DEMPSEY. I think you're right, Congressman. I think that it is very hard to think of a case where agents have been disciplined, and the case you refer to with the FISA court, of course, I think that that issue was addressed in the PATRIOT Act, as well, in a way that that agent would no longer be doing anything wrong for what he did in those cases before the FISA court.

Mr. FLAKE. Is that some good faith exemption because of him, or——

Mr. DEMPSEY. No, that has—I mean, I think the issue there had to do with what was at the time believed to be the primary purpose

test. My understanding of it is that that agent was claiming that there was no criminal interest in the subject when, in fact, there was. Now, the fact that there's a criminal interest in a subject, a FISA court can still grant the order. That was sort of a strange by-product of the way that the FISA got misinterpreted pre-PATRIOT Act.

Mr. FLAKE. When there are provisions in the PATRIOT Act which really require the court or the judge of jurisdiction or whomever, that they shall issue a warrant of some type, that it really is incumbent on the Department or the agency to police their own to make sure that individuals are not filing misleading affidavits. If there is one example that we know of here, and the agency, the Department has taken no action at all, then that doesn't inspire much confidence on the part of Members here that the agencies and the Department can police their own. So I would just bring that up.

Mr. DEMPSEY. Congressman, and again, this partly goes to an issue that I know you're concerned about, which is the issue of notice——

Mr. FLAKE. Right.

Mr. DEMPSEY.—which is how is anybody ever going to know that there's been a violation if they haven't been told, and even the Frank amendment to the PATRIOT Act would almost never get invoked and there would be no discipline unless somebody complained. And if the person whose privacy has been compromised is never told that the Government has accessed their information, there is no complaint, no remedy, no consequences.

Mr. FLAKE. Now specifically—oh, go ahead.

Mr. MOSCHELLA. Mr. Flake, while I don't know the specific disposition of that particular pre—my recollection was that was a pre-PATRIOT Act series of affidavits, I can tell you that the Department does review these matters and does take action. There was a rather highly publicized case in which, in a prosecution, the Department learned that certain materials were not provided to the defendant and on the Department's motion vitiated the prosecution in conviction. We do take these things seriously. We follow the law. We instill some training, the need to follow the rule of law, and it is absolute high priority for the Department.

Mr. FEENEY. The gentleman's time has expired. I do believe we are going to try to have another round, Congressman.

Mr. FLAKE. I thank the Chairman.

Mr. FLAKE. The gentleman from Michigan is recognized.

Mr. CONYERS. Thank you, Mr. Chairman.

We have an interesting situation here. Two former Judiciary staffers, Moschella and Dempsey. We trained you guys. [Laughter.]

One says, no checks and balances are needed in this provision. Let's just reinstitute it and let it go. The other at the other end of the table says, well, there's got to be some safeguards put into this situation.

Now, we just checked what the definition of emergency is, if you could call it a definition. Death or physical injury. Well, that could happen in anything. I mean, for that to be—that is not a serious judgment. What section is that in—section 2701.

Now, I ask you, what's with this emergency provision, Mr. Dempsey? We're living in an age of Blackberries, faxes, e-mails, everything. I mean, it's not like you're on a desert island and you've got to make this judgment real quick. Anything can bring about injury. We could be talking about a misdemeanor.

So with the greatest respect for the Ashcroft PATRIOT Act, which was substituted—which substituted the Judiciary Committee's PATRIOT Act in the Rules Committee that awful night, what's with the emergency provision? We have, I think, implied good faith exceptions running throughout this. If they're not implied, they're used in real life situations. And we changed the reasonable belief proposition for emergencies to good faith. We've lowered the standard. So who would get injured or killed or put in harm's way if this provision in a thoughtful discussion and study of the Subcommittee and full Committee of Judiciary, we dropped it.

Mr. DEMPSEY. Again, Congressman, I'm actually going to argue in favor of keeping this provision. I agree——

Mr. CONYERS. But I want to know—I know there's a great argument in favor of keeping it, but what harm would come if we didn't keep it?

Mr. DEMPSEY. I think there are—and I'm going to make the Justice Department's case for it here—I think there are circumstances that are true emergencies, and what we try to do in this provision is we try to come up with the right set of words that would narrowly define it. In fact, if you go back to the PATRIOT Act provision, it talked about immediate.

Mr. CONYERS. Okay. Give the——

Mr. DEMPSEY. And immediate was dropped, and we've gone back and forth——

Mr. CONYERS. Give me not ten or five, give me one example of a good faith emergency that would be disadvantaged if this provision—if the PATRIOT Act—if this were sunsetted. Describe something to me. Don't point to Moschella. You two were both trained together, so I don't want you playing us off, as they say, now that you're back before the Committee on the other side. No, there isn't any, that's why.

Mr. DEMPSEY. No, I think, again——

Mr. CONYERS. There isn't any that you can't immediately get your order without terming it an emergency. Life is, everything's an emergency in criminal justice.

Mr. DEMPSEY. Well, that I agree with at some level, Congressman, which is why I say we need to look at these other checks and balances. When you're in the heat of the investigation, every case is a priority.

Mr. CONYERS. Of course.

Mr. DEMPSEY. I agree with that. But some of them really are. You may think that they all are, but some of them really are. And I think if you scratch some of these cases, they prove not to be as serious——

Mr. CONYERS. Of course they don't——

Mr. DEMPSEY. But some of them are, I think.

Mr. CONYERS. Well, I know you think that, but that's why you cannot give me one example. Everything is an emergency. You

don't need to write in something this broad and then have the Department of Justice tell you, we don't want any checks or balances.

Mr. FEENEY. The gentleman's time——

Mr. CONYERS. Against some checks or balances or none, I'm for dropping this provision.

Mr. FEENEY. The gentleman's time has expired, mercifully for some of the witnesses, but, Mr. Moschella, in fairness, whether it's real or a genuinely good faith hypothetical, do you have any response to some very penetrating questions that Mr. Conyers asked about why this provision and a definition of emergency may be appropriate or not?

Mr. MOSCHELLA. Well, Mr. Conyers cited to the statute and the statute specifically talks about death or serious physical injury, not just any old emergency, and I would submit that the examples in our testimony are examples where delay could have resulted in death. I did not explain the case of the 88-year-old woman who was kidnapped in Wisconsin. This is a case, I think it may have been in Chairman Sensenbrenner's district or it was near to his district. She was kidnapped, and we had information that we knew if we went to the ISP they would help us locate this individual. She was put in a shack during the winter, in the cold winter in Wisconsin. Luckily, she did not die. It was a freezing cold series of four nights, and we were able to save her.

Mr. CONYERS. Without this provision, she would have died?

Mr. FEENEY. Reclaiming my time, I don't think the witness testified to that, but did say that there was the potential for damage, and also in or near the gentleman from Michigan's district, we had the issue with the mosque that the FBI identified a threat to, but only because they had the emergency access to the ISP, as I understood it, where they were able to identify the two individuals engaged in the potential threat to kill the Imam and others practicing at the mosque. Am I under the wrong impression, Mr. Moschella or—Mr. Hulon, go ahead.

Mr. HULON. Yes, sir. Actually, those examples are examples of emergencies where we did use that provision of the statute to get the information very quickly and respond. And when you're dealing with a situation like that where you have a threat of death or bodily injury, if there is an opportunity for us to get that information and move on it very quickly without delay, then that's in the benefit of the Government as well as the potential victims.

Mr. FEENEY. But in fairness to Mr. Conyers's question, the truth is, we can't prove that but for section 212 there would have been this death to the 88-year-old or the Imam or anybody else. It's just that there potentially was enhanced death threat.

Mr. MOSCHELLA. Mr. Feeney, I don't know that to a metaphysical certitude. What I can tell you is that when the FBI went into this home in Herndon and found a 13-year-old girl chained up in the bedroom of the sexual trafficker, the individual who traveled with the young child, does anyone reasonably believe that he was not—that she was going to be damaged even further? I don't think anyone could reasonably come to any conclusion but that.

Mr. CONYERS. Chairman——

Mr. FEENEY. In deference to—I have a great amount of respect. I will yield briefly if you won't take too much of my time.

Mr. CONYERS. One sentence, Chairman Feeney, referencing the Michigan case. Bratisax and Barnett have been arraigned and charged with the Federal crimes of obstructing the free exercise of religious beliefs and transmitting threatening communications in interstate commerce. Now tell me about the emergency involved in those acts, assuming they were found guilty.

Mr. FEENEY. I'm going to let you follow up in writing on that because I've got a limited amount of time, and I, out of respect, wanted to let the Ranking Member ask his question.

Now, Mr. Moschella—actually, Mr. Kerr, Mr. Dempsey does make some good points. If I'm, for example, typing stuff on my computer, perhaps over the Internet, then there is this theoretical question. Is it more like writing stuff in my own personal diary or is it more like speaking in the public square. The one example we had today was somebody attended a party and overheard conversations about some imminent threat to do violence.

Isn't it appropriate at some point that if somebody's Internet communications have been, for example, appropriated by the FBI legitimately under 212 but they turn out to be a false alarm, aren't I entitled to find out at some point if I was the person that typed that language in, that the Government now has some of my personal thoughts, communications, et cetera, because, right now, there's no provision in 212 to notify anybody ever, is there?

Mr. KERR. Right now, there is no notice provision outside of—well, there are a couple of notice provisions. One would be in the wiretap context following a wiretap where the Government needs to inform the people——

Mr. FEENEY. I'm talking about the computer example.

Mr. KERR. That would apply. I believe it applies also in the Internet context——

Mr. FEENEY. Or stored.

Mr. KERR. For example, Government access to stored Internet communications pursuant to less process than a warrant does require prior notice. There are some notice requirements.

To be honest, I think it's a difficult problem. The traditional fourth amendment model is very light on notice. There's not a lot of paperwork in traditional fourth amendment law. When the Government gets a warrant, of course, that's a separate story. Issuing a subpoena will provide notice to whoever receives the subpoena. The law hasn't traditionally done that, but maybe should do more in the electronic communications context.

Mr. FEENEY. My time has expired and I recognize the Ranking Member of the Subcommittee, Mr. Scott. I'm sorry, actually, the Congressman from Texas, Ms. Jackson Lee, you're recognized. A moment ago we didn't have anybody that hadn't asked on that side, so Congresswoman Jackson Lee, you're recognized.

Ms. JACKSON LEE. Thank you very much, Mr. Chairman.

Let me be—the testimony of the witnesses, and thank you for your indulgence. There is a matter on the floor that I had to debate. But the witnesses' testimony, I am not going to probe specifically as to the comments of your testimony as much as I am going to probe the Achilles heels or the failings of section 212.

Let me just, for framework, just enunciate that as I read it, section 212 allows a phone company or Internet service provider to

give communication records and content to the authorities in emergency situations. The emergency situation does not have to be terror-related, and in fact, all of the examples that the Justice Department has related to us are dealing with ordinary crimes and kidnappings and bomb threats.

It is imperative that we come together, as we did after 9/11, to deal with the idea of homeland security. But the word "emergency" and no definition disturbs me.

The PATRIOT Act, for many of us, is an extension of powers, powers that this country already had. One of, I think, the more serious aspects of being safe is the collection of intelligence. That's where I think the most important focus is. These various provisions are allegedly to contribute to collecting intelligence. At the same time, there is no bar to use them for any myriad of reckless, random activities that may or may not provide for the security of this nation.

We are a nation of laws. We need to enforce them. We need to protect our nation. But we're also a nation of civil liberties and balance.

Mr. Dempsey, you said that there is a place for the PATRIOT Act, and I would agree with you. There is a place for the PATRIOT Act that this Committee worked through and passed out of Committee unanimously. Mr. Sensenbrenner, Mr. Conyers, and the entire body voted for the PATRIOT Act, from conservatives, if you will, to progressives, because we understand reality.

I'm going to ask a question across the board. This broad term emergency, not defined, may be ultimately defined by court cases, seems to be overbroad and undefinable. Emergencies can be of any kind. Emergencies can be because I don't want to bother to go through the normal traditions of seeking a PC, getting a probable cause, and getting a warrant. Emergencies can be because I'm overworked. Emergencies can be because I'm understaffed. Emergencies can be because I don't like these guys. Emergencies can be because they practice a different religion from the general population. Emergencies can be because their neighbor next door is a problem. Undefinable and dangerous, from my perspective.

So I'll start with Mr. Dempsey. Where do we narrow the focus, and am I highlighting the problem, and is 212 fixable?

Mr. DEMPSEY. I think you're right on target and I think that 212, like every other provision of the PATRIOT Act, is fixable. But I've ended up at this hearing arguing with my good tutor, the Ranking Member of the Committee, because the Justice Department, and I've been defending the PATRIOT Act here, but they've been unwilling to come forward and talk about and engage on these checks and balances. They want the authority, and every one of these, in my view, has a legitimacy to it, but they don't want to engage on the issues that the Members of this Subcommittee and of the full Committee across the board in 2001 and now again want to engage on. How do we build in accountability? How do we build in oversight? Tell us exactly how many times——

Ms. JACKSON LEE. And I'm going to allow him to do that because my time is short. You've raised a probative question. Mr. Moschella and Mr. Hulon and Mr. Kerr, let me just simply say, I want to give you the tools, but I come from a history where laws have been used

against populations like the one I happen to belong in, one, an American, but also an African American, and we notice that the laws are used not from a terrorist perspective, but certainly adversely to our population in the '60's and the '50's and the early 1900's.

Let me, Mr. Moschella, are you willing to look at the points, or the Justice Department, at the points of concern that are being raised, I guess by this Committee, maybe on both sides of the aisle, in terms of the looseness of 212 and the ability for this to be, if you will, a fishnet to see what we can haul in?

Mr. MOSCHELLA. I'd like to make a couple of points. The first is to reiterate what the Attorney General said at the full Committee hearing. He said that he wanted to listen to criticisms and engage in that discussion, and if there were things that needed to be fixed, he is certainly open to doing that.

With regard to your specific question about whether emergency is so broad, the statute specifically says that the emergency must involve the immediate danger of death or serious physical injury, so I would respectfully disagree that it is too broad.

I'd also make this point, and I think Professor Kerr's written testimony is instructive. In his testimony, he talks about exigent circumstances and he views this emergency provision as, in a way, coextensive as the exigent circumstances doctrine in fourth amendment jurisprudence. Actually, this is much narrower because it only deals with danger to life and limb. He has a quote in his testimony from a Ninth Circuit case, which I won't read to you. I would just point that out, that this is even narrower than the exigent circumstances exception that we find in fourth amendment law.

Ms. JACKSON LEE. The question is the perception that is given to those definitions. There can be a myriad of perceptions by law enforcement officers attached to murder and threat, and there is no defined criteria to make those determinations.

Mr. Hulon?

Mr. LUNGREN. [Presiding.] The gentlelady's time has expired.

Ms. JACKSON LEE. I thank the gentleman. I had asked Mr. Kerr and Mr. Hulon. Is it possible to ask unanimous consent for them to answer the question, answer that question?

Mr. LUNGREN. You can ask unanimous consent. Okay. So ordered.

Ms. JACKSON LEE. Thank you very much for your courtesies, Mr. Chairman and colleagues.

Mr. HULON. Thank you. In regards to your question about emergencies and the fact that the statute has not been used for terrorism, it has been. The example that I gave of the threat to burn down a mosque, I mean, that's considered terrorism just like the threat to the mosque in Detroit as well as the Imams. Those are strictly—those are emergencies where there is a threat to do bodily harm or to kill individuals that we would address under the terrorism program.

So I would say that when we do that, we're looking at using this statute to respond where there is an immediate threat so that we can get there and respond to that crisis. And when you're talking about responding to a crisis, minutes add up. In the meantime, we

can say, well, we have a statute or we have a provision that we can use. We would do that.

And we do use that statute or that provision diligently and not abuse that, and the examples we gave were in regard to responses that had to do with life and death, just like the example I gave of Mrs. Stinnett. I mean, she was already dead and murdered, but her child was still alive and that child was recovered. That was not a terrorism case, but that was one that really merited us responding quickly. Thank you.

Ms. JACKSON LEE. Mr. Kerr?

Mr. KERR. I'll just respond briefly. The text of section 212, I think, is quite narrow. The idea of an emergency involving only death or serious bodily injury is quite narrow. The exigent circumstances exception, in contrast, is extremely broad, some of the language used. Some consequence in properly frustrating legitimate law enforcement efforts can justify an exigent circumstances search. So that's quite broad and the statutory language here is actually much narrower by comparison.

I think in terms—if the concern is that courts may construe that language more broadly, or worse, law enforcement may construe it more broadly, I think the answer is some sort of statutory suppression remedy that puts the issue before a court and allows a court to further define what that language actually means.

Ms. JACKSON LEE. Thank you. Mr. Chairman, I conclude by just saying that the Barnett-Bratisax case—basically, Mr. Hulon, they're being charged with free exercise of religion, or obstructing the free exercise of religion and they are waiting on trial, and so—and transmitting threatening communications in interstate commerce. I'd just simply say that judicial review would be warranted, I think, and I don't think—I've given PCs, and I haven't been on the Federal bench, but I've given probable cause warrants at 12 midnight as a judge in Houston, Texas. I know we can act quickly and I just don't see why we should not have that provision and use it usefully here.

I yield back, Mr. Chairman. Thank you.

Mr. LUNGREN. The gentlelady's time has expired.

I'll take 5 minutes now. Mr. Moschella, I'm not concerned about the narrowness of the scope of this particular emergency provision. It seems to me you can't get much narrower than immediate and life or limb. But what I am concerned about is no judicial review whatsoever, as I understand it, under these—I'll call them exigent circumstances.

What would be the harm in requiring some review by a court after the fact as a means of assuring those who are concerned that this exceptional power, and it is an exceptional power, I think we have to recognize that. I mean, I think we have—I realize constitutionally we don't have the expectation of privacy, but most people, I think, have an expectation of privacy of their stored communications being held by a third party. In fact, most people don't really understand how it all works. They think it's in their machine.

What would be the problem with requiring, and I don't know how we would define it, within a reasonable period of time or within a certain number of days or at the conclusion of the investigation, an application to the court at that time for the court to review it, and

at that time, if it showed that there was information of a third party that somehow had come to the attention of the Government, that the court could make the determination as to whether that third party ought to be given notice that their information had been, quote-unquote, exposed to the eyes of the Government?

Mr. MOSCHELLA. Well, in this circumstances, Mr. Chairman, I'm not sure which court one would go to. In the grand jury context in which a U.S. Attorney is subpoenaing similar sorts of records from a bank, for example, and these are the same—the expectation of privacy is just about the same in the physical world as it is in the online world in these cases. We're not reporting back to the judge every time we get a return on a grand jury subpoena. Again, I don't——

Mr. LUNGREN. No, but this is an extraordinary circumstance, as you recognized. We're giving an extraordinary grant of power, which I think is appropriate because we're talking about very few circumstances. If that's the case and there is the concern that arises from others that, as much as I appreciate law enforcement, we're not perfect. I had my disagreements with the FBI when I was Attorney General in terms of certain investigations and so forth, although I think we're all trying to do the right thing, but we make mistakes.

Because we're talking about something that's very, very important, the concern that people have about Government getting too intrusive, too large, what's wrong with having some sort of mechanism by which at least we have the interposition of a third party that is a magistrate, a judge, to take a look at it after the fact to see if, in fact, it was appropriate, and also to make the judgment as to whether or not someone ought to be given notice that their information has been viewed by the Government, not that they would do it in all circumstances, but the judge would make that determination.

Mr. MOSCHELLA. Well, we certainly would want to take a look at whatever proposal came up. I just want to make this point. The records that we're talking about, for example, basic subscriber information, there is little expectation of privacy—it's information that we obtain via subpoena in countless cases on a daily basis and I don't——

Mr. LUNGREN. But this is not done pursuant to subpoena, correct?

Mr. MOSCHELLA. No.

Mr. LUNGREN. What we're talking about here is outside of subpoena.

Mr. MOSCHELLA. Well, in the emergencies, that's correct.

Mr. LUNGREN. That's all I'm talking about, emergency scenario here.

Mr. MOSCHELLA. Well, but in the subpoena context under ECPA, we're not going to the judge. There are some categories of records under ECPA that a court order is necessary with differing standards, whether it's relevance or whether it's probable cause. But in the case of subscriber information, for example, a mere subpoena would suffice.

Mr. LUNGREN. I don't think I heard an answer from you about whether or not the Administration would be opposed to considering the suggestion I made.

Mr. MOSCHELLA. We certainly would consider it.

Mr. LUNGREN. Mr. Dempsey, what do you think about that kind of an approach?

Mr. DEMPSEY. I think you're right on track. That's very similar to the process that occurs in emergencies under title III and it does provide that sort of—you accommodate the emergency, you save the life, but it gives you that oversight, that judicial oversight, in cases where there was a mistake or where there was some overreaching, and that's all we're talking about here.

Mr. LUNGREN. Thank you very much. My time has expired.

Mr. Delahunt?

Mr. DELAHUNT. Thank you, Mr. Chairman. You anticipated my own line of questioning.

Mr. LUNGREN. I was just trying to shorten the gentleman's time.

Mr. DELAHUNT. I appreciate that, but I'll try to fill it up anyhow. [Laughter.]

I mean, the reality—let's be practical. I mean, the Frank amendment, I supported it. It was well intentioned. But for a citizen to sue the Government, it's extremely rare. It requires an extraordinary amount of resources that most people simply don't have. So, with all due respect.

And we have a history in various investigatory agencies of conduct that is unacceptable. I mean, I was unaware that in a FISA application, was it an FBI agent that has been excluded from appearing before the FISA court again? Was that an accurate——

Mr. MOSCHELLA. This is very, very old news. This is quite some time ago——

Mr. DELAHUNT. No, I'm not suggesting—it's new news to me, and I'm not trying to get into it, but what I'm saying is it's evidence that, on occasion, there are problems, and that's what we are trying to speak to in terms of talking about the concepts of checks and balances, because we vest such incredible authority in those who are conferred the authority to invade other people's privacies under the color of law.

So while these instances hopefully are rare, I believe it's our responsibility to ensure that there is as much accountability and transparency as possible without jeopardizing our national security. And again, I look to these provisions, and I think some of them, clearly, they have a certain legitimacy. But we're now at a different point. Now, we can go back and examine and think of what is necessary to secure the confidence of the American people in terms of what we did, and I think that's what you're hearing on this side up here.

You know, I listened to both Mr. Dempsey and Professor Kerr. What's the problem with a statutory exclusion? Mr. Moschella?

Mr. MOSCHELLA. You mean a statutory suppression remedy?

Mr. DELAHUNT. Exactly.

Mr. MOSCHELLA. Well, there certainly is for any constitutional violation——

Mr. DELAHUNT. I'm not talking about a constitutional violation.

Mr. MOSCHELLA. Right. I just want to point out that is available.

Mr. DELAHUNT. I understand it. I'm talking about a statutory suppression provision.

Mr. MOSCHELLA. Well, we certainly would be concerned if the Committee moved in that direction. There are any number of internal mechanisms that we use to address these problems, but——

Mr. DELAHUNT. See, but that's——

Mr. MOSCHELLA. Well, let me say——

Mr. DELAHUNT. Okay.

Mr. MOSCHELLA.—the statutory exclusion would defeat the truth-seeking nature of the criminal process and would only really benefit the criminal defendant.

Mr. DELAHUNT. I have to say, there are some—you know, even in a constitutional fourth amendment exclusionary, I'm sure that what the Founders were considering is the balance of public safety and the balancing of constitutional rights and privacy, and I dare say the same analogy exists here. Hopefully, it would be very, very rare. But we don't—we've proven again and again and again, we don't have those internal mechanisms that operate all the time, that work to a degree that is satisfactory to the American people. That's what I'm talking about.

Mr. Dempsey?

Mr. DEMPSEY. Well——

Mr. DELAHUNT. Before you go, Mr. Kerr, why don't you give us some language? Could you send me some language, statutory language that you think would satisfy the—that would meet the needs that you expressed in your testimony in terms of a statutory remedy?

Mr. KERR. I'd be happy to.

Mr. DELAHUNT. Thank you.

Mr. DEMPSEY. Well, let me say, Congressman, that you always hate to throw out evidence.

Mr. DELAHUNT. Of course.

Mr. DEMPSEY. And I think Congressman Lungren has been concerned about this issue for years and other Members have been, as well. I think on the fourth amendment side, we've reached an uneasy balance, but let's call it a balance, with the good faith exception. But as you were saying, Mr. Chairman, none of that applies in this strange stored e-mail space here and we're sort of the captives of some old fashioned thinking that, "Oh, it's over there so there's no privacy in it." The average person thinks there is.

What the Congress has tried to do is to create with the Electronic Communications Privacy Act that structure of privacy protection. And since 1986, the world has totally moved in the direction of e-mail, Internet, storage, things outside of your office, your home, your laptop, and that's what we're trying to do. We're trying to create similar rules for that environment. Right now, the way 212 works, none of those apply.

Mr. LUNGREN. The time of the gentleman has expired.

The gentleman, Mr. Flake, is recognized for 5 minutes.

Mr. FLAKE. I thank the Chairman, and this won't take 5 minutes, but with regard to what we do this year with regard to the sunsets, would the Department of Justice be adverse to having separate debates and votes on separate provisions that are being sunsetted, or—I mean, that would seem to be a better way to

maybe have the right debate, because as has been pointed out here, all of us on the Judiciary Committee saw the reason for the PATRIOT Act and all of us voted for the version that came out of this. Some of us, including myself, voted for the version that passed on the floor, mostly because the sunset provisions were there and we knew that we could come and revisit it. But if I could get Mr. Moschella's thoughts on that.

Mr. MOSCHELLA. Mr. Flake, as a former Parliamentarian of this Committee and now an executive branch official, I'm not going to tell this body, a separate branch of Government, exactly how it's going to manage its markup. I do want to make this point, though, that the President has called for the reauthorization of the PATRIOT Act and we believe that all 10 provisions need to be reauthorized.

Mr. FLAKE. But there have been—the Attorney General, when he testified before this Committee and before the Senate, conceded that there are some amendments that ought to be entertained, I guess is the way he put it, particularly with regard to the gag order and——

Mr. MOSCHELLA. With regard to section 215, he stated that, number one, the Congress could write in the relevant standard which we believe to be implicit in the statute, the ability to confer with an attorney, and the ability to challenge a 215 order in the FISA court.

Mr. FLAKE. To Mr. Dempsey's point that he made before, it would help us—it would seem that the Department would enjoy more cooperation and have more credibility if there was a little more give and take here and a little more effort to say, all right, that may be more of a problem. Let's look at the ways we can have checks and balances. I see you nodding your head, Mr. Dempsey. Can you comment on that?

Mr. DEMPSEY. I don't understand the either/or nature of this debate: you know, they all sunset or they all have to get renewed as is. We're talking here about the lack of an emergency exception in the Electronic Communications Privacy Act of 1986. That legislation went through months of hearings, markups, considerations, not under the kind of crisis situation we faced in October of 2001, and yet Congress forgot stuff. They left stuff out. They didn't put in an emergency exception. So, of course, come back and fix it.

Now, in 2001, we didn't know if there was going to be another attack. We had the anthrax attacks. The Senate was shut down. We were worried about when the next attack would be and this legislation went through. Of course, mistakes were made. Of course, some of the checks and balances were left out. Now come back, keep the tools, keep the authorities, but put in the checks and balances.

Mr. FLAKE. I'm still a newbie here. This is just my third term. But what I have come to understand with regard to this relationship is that the Department of Justice, as is their role, is to fight terrorism and to fight crime and they will take every tool that is given to them, as they should, apparently. But it's the Congress's role to make sure that there are appropriate checks and balances there and that's what these oversight hearings are all about and

I commend this Committee for having thorough hearings on this matter and thank the witnesses for good testimony.

Mr. LUNGREN. Mr. Dempsey, I would just suggest that your comment about 1986 where we didn't complete a perfect bill, I'm the only Member here who was here in '86——

Mr. DEMPSEY. Yes, sir.

Mr. LUNGREN.—but I will point out I was in the minority at the time. [Laughter.]

Mr. Scott?

Mr. SCOTT. Thank you, Mr. Chairman.

If the information is not used in a criminal investigation, we may not know that it is ever gathered. Mr. Moschella, would you agree that we need a report to Congress so we can get an idea of how much this section is actually being used?

Mr. MOSCHELLA. Mr. Scott, we would be happy to look at any reporting requirement. One thing I want to point out, though, in the context of the intelligence reform bill, Congress imposed, at my count, 106 new reporting requirements. We certainly want to make sure that they're meaningful, they're useful, that they are read, and that the same people who are putting the information together for these are also the same people fighting the war on terrorism and crime.

Mr. SCOTT. Part of the problem is, we don't know how wide a net we're casting when we go to get the information. You may get specific information in a kidnap situation in an emergency, life and limb involved, but that's not—probably not all you're getting. What portion of the information that you get do you actually use in prosecutions?

Mr. MOSCHELLA. I'm not able to answer that question.

Mr. SCOTT. Once you get the information, what limitations are placed on how long it can be retained and who gets to see it?

Mr. HULON. I can respond to some of that, sir. The information that is obtained, I'd like to point out that primarily the information we're talking about obtaining is information in regards to the subscriber or the person who has that account, and what we're looking for, the FBI at that particular time, is the location of that person to try to resolve or prevent a crisis from occurring.

The information that is obtained, of course, is put into the FBI files. It is not disseminated outside to the public. It's——

Mr. SCOTT. It's not disseminated to the public, but last time we checked, this is—is this subject to that information sharing, where you can give it to the FBI and to local law enforcement and the Department of Defense and every public official that works in the neighborhood, some of whom may, in fact, be your neighbors, and some of this information may not be useful in a criminal investigation, but may be embarrassing?

Mr. HULON. Sir, the information would only be used for law enforcement or intelligence purposes. It would not just be provided to a public official. It would be within the intelligence channels as well as——

Mr. SCOTT. Yes, but when you submit it to—when you give it to another agency, these are not robots and computers. These are human beings, some of whom may be your neighbors or my neighbors or the person whose information—and some of it could be po-

litically embarrassing. I mean, you don't have to give it to so many people before somebody, you know, this might be some juicy stuff.

Mr. HULON. Sir, the information that we're talking about here would be the subscriber information to the person that has that Internet service, and when the information is disseminated, it's disseminated for law enforcement use only or for intelligence purposes, and we have requirements as far as how that information can be used and the people that receive that information understand those requirements, too. And so, therefore, that information is still within our channels. It's still protected. It's still guarded.

Mr. SCOTT. Mr. Dempsey, during the commentary and a lot of the discussion and testimony, there was a difference between non-content information and content information. What's the difference statutorily and why should it make a difference?

Mr. DEMPSEY. Well, we're really talking about two emergency exceptions here, one that relates to the content of e-mail storage, and, as we know, Google and Hotmail and others are now offering huge volumes of storage so that you store lots and lots—years worth of e-mail with the service provider. And then the second emergency provision relates to the subscriber identifying information, which we would call the transactional information.

Sometimes, particularly in the Internet context, it's a little bit difficult to draw the line there. I think that the Justice Department's position should be that the "re" line on an e-mail, for example, is content, not transactional. The "to" and "from" line is transactional information. Some of the other——

Mr. SCOTT. But what about my credit card information and billing address? That could be some important information for law enforcement to get. I think——

Mr. DEMPSEY. Those are considered transactional. That's on the non-content——

Mr. SCOTT. That would be the best information. You get somebody communicating back and forth, you don't know where they are. You get the address, that's real good law enforcement information. Where is that in content and non-content, and what difference should it make in terms of what they can get?

Mr. DEMPSEY. Credit card information falls on the non-content side.

Mr. SCOTT. And what difference does it make whether it's content or non-content?

Mr. DEMPSEY. Well, in this case, it makes no difference. I mean, actually, there's some slight wording difference between the emergency exception for content information and the emergency exception for non-content information. One says immediate danger. Ironically, the standard now for non-content information is a little stricter than the standard for content information. Again, that's sort of the somewhat, I won't say sloppy, but that's a byproduct of the way in which these things are drafted.

Mr. LUNGREN. The gentleman's time has expired.

We've got a vote on. I know the gentlelady wants to ask a question to submit to you, if you could then give us the answer in written form.

I just wanted to make one thing clear. I feel strongly that we should look at some judicial intervention. That does not mean I

support a suppression statute here. As one who's worked for 25 years for a good faith exception to the exclusionary rule and realize that sometimes suppression punishes the victim rather than the constable who went wrong, I don't support that. But I think some sort of ability of a magistrate to intervene and also to make a judgment as to whether notice ought to be given.

The gentlelady is recognized to ask her question.

Ms. JACKSON LEE. Let me just say, I want you to have the opportunity to enforce our laws. Judicial review for 212 has to be considered, and I believe it's imperative.

This question is to just ask you to provide for us the steps that the Department of Justice has taken to ensure the more than 70 errors and misrepresentations regarding information sharing, unauthorized dissemination of information which are described in the Foreign Intelligence Surveillance Court's 2002 opinion order so that we know it will not be repeated.

There are too many exceptions to 212. I want you to have the skills. I appreciate—and the tools. But really, I think there needs to be a balance. I thank you for your testimony.

Mr. LUNGREN. I thank the gentlelady.

I'd like to thank the witnesses for their testimony. The Subcommittee very much appreciates your contribution.

In order to ensure a full record and adequate consideration for the important issue, the record will be left open for additional submissions for 7 days. Also, any written questions that a Member wants to submit should be submitted within the same 7-day period.

This concludes the oversight hearing on "The Implementation of the USA PATRIOT Act: Section 212—Emergency Disclosure of Electronic Communications to Protect Life and Limb." Thank you for your cooperation. The Subcommittee stands adjourned.

[Whereupon, at 11:50 a.m., the Subcommittee was adjourned.]

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

PREPARED STATEMENT OF THE HONORABLE ROBERT C. SCOTT, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF VIRGINIA, AND RANKING MEMBER, SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

Thank you, Mr. Chairman. And I want to again express my appreciation to you for devoting the time and attention you have to the issue of sunsetted provisions under the USA PATRIOT Act by holding the series of hearings you have held on the provisions, including this hearing on Section 212, which involves emergency disclosures under the Act.

What the hearings have revealed to me is the extent to which we have authorized unchecked and indiscriminate secret access by the government to private, confidential, citizen communications and information. With section 212 and other provisions we have effectively changed provisions designed to protect private information from disclosure without due process, to provisions designed to allow or require indiscriminately disclosure of information to the government. And such disclosures can be made with virtually no detached oversight or any other checks and balances such as requiring notice before or after the fact, requiring reporting to either a court, the Congress or the public, or requiring sanctions or remedies for wrongful acts or abuses.

Moreover, with the liberal information sharing provisions we have authorized, this secretly acquired private, confidential information can be spread all over town without the person to whom the information pertains ever knowing anything about it. Further still, there are absolutely no restrictions on how long, or by whom, the information can be maintained.

I expect that we will again here from the Department of Justice and others how important it is for the government to have secret, virtually unfettered access to our private, confidential information in order to protect us from terrorism or eminent threats to our health safety. However, we are not likely to hear how many times the authorities have been used where no terrorism or eminent threat was involved or how many times no criminal proceedings or other actions ensued to show the intrusions were warranted. We are left to simply trust government officials to always do the right thing at the right time in the right way, with complete impunity, and without the bother of a court, the Congress, or the public, looking over their shoulder while they are doing it.

Mr. Chairman, we should use the information we have gleaned on the extraordinary secret powers we have authorized, to put in ordinary checks and balances such as notice, court oversight, reporting requirements and sanctions and remedies. To fail to do so would turn on its head not only the Electronic Communications Privacy Act (ECPA), and intent of the Forth Amendment to the Constitution, but the healthy mistrust of government the Framers of our system intended, as well.

So, Mr. Chairman, I look forward to the testimony of our witnesses on how these extraordinary powers are being used and how we can best provide for the necessary checks and balances our system calls for, and to working with you to implement them. Thank you.

PREPARED STATEMENT OF THE HONORABLE JOHN CONYERS, JR., A REPRESENTATIVE IN CONGRESS FROM THE STATE OF MICHIGAN

Today we're here to discuss one of the many criminal provisions in the PATRIOT Act that has nothing to do with terrorism. As these hearings have highlighted, some in our government used the tragedy of 9/11 and the fear of terrorists in the immediate aftermath to ram through new powers to investigate every day crimes.

First, I am concerned that this provision, sold to this Congress as a way to protect our critical infrastructure from terrorists, has been a boon to cops seeking information on every day crimes. Truly, sidestepping the court system completely can only be done in the gravest of circumstances—and this section of the PATRIOT Act is not limited even to cases where danger is immediate. It goes to far and in too many cases, especially in cases that have absolutely nothing to do with terrorism.

Second, there are no safeguards to ensure that those who scare internet and phone companies into turning over their customer's information are doing so only when spending that extra hour to get a warrant is truly impossible. There are not even safeguards after the fact, and plainly, there is no justification for avoiding judicial review or notice to the target after the so called emergency is over. Indeed, we afford that courtesy to suspected terrorists under the Foreign Intelligence Surveillance Act after an emergency order is not extended by the FISA court. I would hope that we would extend the same rights to American citizens suspected of far less serious crimes.

Third, the Justice Department has yet to come forward to explain how this section has helped prevent terror attacks or saved a single life or limb from terrorists. We will hear anecdotes today about everyday kidnappings and computer hackers—but anecdotes are not oversight. I hope to hear whether Section 212 has truly been used to combat terrorism, or merely rode into law on terrorism's coattails.

Finally, hearing after hearing, we are told that these changes to Title 18, our criminal code, are necessary to prosecute terrorists. Yet, the list of actual convictions is horribly small. We've rewritten our criminal laws and compromised the 4 th Amendment all for the sake of putting terrorists behind bars—because that is the sole purpose of our criminal code—and it has been a failure. As we go forward and discuss all the criminal provisions in the PATRIOT Act, we must decide whether a handful of guilty pleas are worth compromising the rights of the entire citizenry.